NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

TEST AND EVALUATION OF A PROTOTYPED SENSOR-CAMERA NETWORK FOR PERSISTENT INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE IN SUPPORT OF TACTICAL COALITION NETWORKING ENVIRONMENTS

by

Michael R. Chesnut

June 2006

Thesis Advisor:	Gurminder Singh
Co-Advisor:	James Ehlert

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	June 2006	Master's Thesis

4. TITLE AND SUBTITLE Test and Evaluation of a Prototyped Sensor-Camera Network for Persistent Intelligence, Surveillance, and Reconnaissance in Support of Tactical Coalition Networking Environments

5. FUNDING NUMBERS RIS57

6. AUTHOR(S) Michael R. Chesnut

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Space and Naval Warfare Systems Center
San Diego, CA

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

This thesis investigated the feasibility of deploying an integrated sensor-camera network in military and law enforcement applications. The system was built using entirely commercial-off-the-shelf technologies. The prototype used the unattended ground sensors combined with digital video surveillance cameras to provide accurate real-time situational awareness, persistent intelligence and remote security.

A robust testing and evaluation plan was created to measure the system's performance based on specific metrics. The tests focused primarily on the capabilities of the sensor aspect of the network. Tests were conducted to determine the maximum detection range, probabilities of detection, maximum communications range, and battery life. Mathematical models were created to assist network planners. Additionally, the prototyped system was tested through field exercises as part of the Naval Postgraduate School's Coalition Operating Area Surveillance and Targeting System field demonstrations in California and northern Thailand. Although the sensing capabilities exceeded the minimum metrics, the system was not suitable for use in military applications. However, the prototyped network would work well in less demanding law enforcement environments. Additionally, the feasibility and the need to develop an integrated sensor-camera network were demonstrated.

14. SUBJECT TERMS Integrated Sensors, Surveillance, Digital Video, Metrics, Coalition Networking, Prototype, Test and Evaluation

15. NUMBER OF PAGES 258

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

TEST AND EVALUATION OF A PROTOTYPED SENSOR-CAMERA NETWORK FOR PERSISTENT INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE IN SUPPORT OF TACTICAL COALITION NETWORKING ENVIRONMENTS

Michael R. Chesnut
Ensign, United States Navy
B.S., United States Naval Academy, 2005

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY
(COMMAND, CONTROL AND COMMUNICATIONS (C3))**

from the

**NAVAL POSTGRADUATE SCHOOL
June 2006**

Author: Michael R. Chesnut

Approved by: Gurminder Singh
Thesis Advisor

James Ehlert
Co-Advisor

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis investigated the feasibility of deploying an integrated sensor-camera network in military and law enforcement applications. The system was built using entirely commercial-off-the-shelf technologies. The prototype used the unattended ground sensors combined with digital video surveillance cameras to provide accurate real-time situational awareness, persistent intelligence and remote security.

A robust testing and evaluation plan was created to measure the system's performance based on specific metrics. The tests focused primarily on the capabilities of the sensor aspect of the network. Tests were conducted to determine the maximum detection range, probabilities of detection, maximum communications range, and battery life. Mathematical models were created to assist network planners. Additionally, the prototyped system was tested through field exercises as part of the Naval Postgraduate School's Coalition Operating Area Surveillance and Targeting System field demonstrations in California and northern Thailand. Although the sensing capabilities exceeded the minimum metrics, the system was not suitable for use in military applications. However, the prototyped network would work well in less demanding law enforcement environments. Additionally, the feasibility and the need to develop an integrated sensor-camera network were demonstrated.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ABBREVIATIONS AND ACRONYMS

ANOVA	Analysis of Variance
BPSK	Binary Phase Shift Keying
BS	Base Station
C2	Command and Control
CCA	Clear Channel Assessment
CCD	Charge-Coupled Device
CH	Cluster Head
CID	Cluster Identifier
COASTS	Coalition Operating Area Surveillance and Targeting System
CONOPS	Concept of Operations
COTS	Commercial-off-the-Shelf
DC	Direct Current
DCT	Discrete Cosine Transform
DSSS	Direct-Sequence Spread Spectrum
DVS	Dynamic Voltage Scaling
EAR	Eavesdrop and Register
ED	Energy Detection
ESG	Expeditionary Sensor Grid
FCC	Federal Communications Commission
FCS	Frame Check Sequence
FFD	Full-Function Device
FLAK	Flay-Away Kit
GHT	Geographic Hash Table
GPS	Global Positioning System
IEEE	Institute of Electrical and Electronic Engineers
ISM	Industrial, Scientific, and Medical
JPEG	Joint Pictographic Experts Group
KDD	Knowledge Database Design
LEACH	Low-Energy Adaptive Clustering Hierarchy
LED	Light Emitting Diode
LLC	Logical Link Control
LLNL	Lawrence Livermore National Laboratory
LQI	Link Quality Indication
LR-WPAN	Low Rate WPAN
MAC	Medium Access Control
MFR	MAC Footer
MHR	MAC Header
MIC	Message Integrity Code
MIO	Maritime Interdiction Operations
MoE	Measure of Effectiveness
MoP	Measure of Performance
MPEG	Moving Pictures Expert Group

NPS	Naval Postgraduate School
OSI	Open System Interconnection
PAN	Personal Area Network
PDA	Personal Digital Assistant
PHY	Physical Layer
QPSK	Quadrature Phase Shift Keying
RF	Radio Frequency
RFD	Reduced-Function Device
RFID	Radio Frequency Identifier
RGB	Red Green Blue
RTS/CTS	Request-To-Send/Clear-To-Send
SMACS	Self-Organizing MAC for Sensor Networks
SPIN	Sensor Protocols for Information via Negotiation
SSCS	Service Specific Convergence Sublayer
SURAN	Survivable Radio Network
TCP/IP	Transmission Control Protocol/Internet Protocol
TDMA	Time Division Multiple Access
UAV	Unmanned Aerial Vehicle
UNPF	Unified Network Protocol Framework
WINS	Wireless Integrated Network Sensors
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Network

ACKNOWLEDGMENTS

I would like to dedicate this thesis to my family for all of their support, hard work, and willingness to assist me. Without them I would not be who I am today. Thank you for all that you have done, are doing, and continue to do.

I would like to thank LTC Andy Hernandez, USA, for his immense support during this process. Without his assistance, the testing process would not have been nearly as sound or rigorous. His capabilities and willingness to assist have helped to create a robust testing plan and ultimately an evaluation of the network. He greatly helped me achieve my goals during this project.

Finally, I would like to thank my two advisors, Mr. James Ehlert and Dr. Gurminder Singh. Without their guidance and assistance, this project would never have gotten off of the ground. Thank you very much.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The documents shaping the United States national military strategy call for the use of emerging information technologies as a force multiplier to produce a more agile, flexible, and effective military that can respond to an increasingly asymmetric enemy. Joint Vision 2020 recognizes the role of unattended sensor networks in full-spectrum dominance by increasing battle-space awareness and precision engagement. Likewise, Sea Power 21 calls for persistent intelligence, surveillance, and reconnaissance operations using unattended ground, air, and sub-surface sensor grids. These documents led to the development of the Expeditionary Sensor Grid (ESG) concept. The ESG will provide real-time sensor coverage using hundreds to thousands of fully networked, low-power, plug-and-play nodes with long battery lives. The ESG aims to increase military effectiveness and efficiency by fusing sensor data seamlessly through the strategic, operational and tactical levels of US and Coalition forces.

Although the concepts of wireless ad-hoc networks and infrastructure-less communication have been investigated and researched for several decades, the wireless sensor network subcategory is relatively new. Wireless sensor networks consist of interconnected devices embedded in larger systems or environments. Their capability to observe and interact with the environment accurately in "real time" suggests numerous applications in the research, industrial, and military communities.

The emergence and relatively low cost of commercially available wireless networking technologies, which support traditional peacekeeping, law enforcement, and non-governmental organization applications (such as humanitarian assistance and disaster relief), create potentially important operational and resource considerations for decision-makers. Previously, the implementation of wireless sensor networks for military and law enforcement purposes was not feasible due to the lack of commercially available equipment and the constant monitoring and substantial processing needed. Improvements in sensor-network technology continue to decrease size, cost, and weight of sensors while increasing their reliability and the capabilities of the sensors. However, many technological challenges and limitations associated with operational military and

law enforcement applications remain. Exploiting the true capabilities of an integrated sensor network can greatly benefit military and law enforcement agencies.

A. OBJECTIVES

Recent theoretical and simulation studies have provided a basis for implementing integrated sensors to detect, classify and track objects. Even though these studies provide sufficient background, a more in-depth study is needed to determine the feasibility of deploying such technology in real-life military and law enforcement scenarios.

The objective of this thesis is to undertake a system level test of commercially available integrated sensors and IP cameras to assess the networks capability to detect, classify, and to track anomalous events in a variety of military scenarios. Specific performance metrics include radio and sensor range, detection probabilities, battery life, and sensor elevation.

Using the IEEE 802.15.4 protocol and Commercial-off-the-Shelf-Technology (COTS), a prototyped sensor-camera network was developed. The network consisted of a Crossbow MSP410CA integrated sensor suite and Axis network IP cameras. Measures of Effectiveness and Measures of Performance, discussed in detail in subsequent chapters, were created to compare the test results and to determine the effectiveness and feasibility of deploying the system in real-world military and law enforcement environments. The networks radio range, sensor range, and capabilities were measured in numerous operating conditions.

B. RESEARCH QUESTIONS

The primary research question explores the optimal configuration of an integrated sensor-camera network to detect vehicular traffic. Additionally, this thesis focuses on determining the true capabilities of the network under varying operational environments and meteorological conditions. Secondary questions include, but are not limited to:

1. Will 802.15.4 maintain connectivity in an adverse, high-temperature, high-humidity environment?
2. What is the maximum effective detection range of Crossbow sensors in varying environmental conditions?

3. How does the elevation of the sensor affect detection range?
4. How can Crossbow sensors be employed to classify various objects?
5. What are the probabilities of detecting objects traveling through a sensor grid?
6. How does the physical topology affect sensor capabilities?

C. SCOPE

The principal research consists of several system-level tests and evaluates a prototyped sensor-camera network. The primary objective is to determine the optimal configuration of an integrated sensor-camera network to detect vehicular traffic. To accomplish this objective, a robust test and evaluation plan is produced. Using this test plan, the system is base-lined in the moderate operating conditions of Monterey, California. The system is then tested in various operating environments to include, but not limited to, California (Point Sur, Fort Ord, and Fort Hunter-Liggett) and northern Thailand as part of the Naval Postgraduate School (NPS) Coalition Operating Area Surveillance and Targeting System (COASTS) field experimentation program from late CY2005 through mid-CY2006.

D. METHODOLOGY

The methodology consisted of extensive research of available literature, both hard copy and electronic, as well as extensive testing and evaluation of the prototyped sensor-camera network. The research methodology was divided into the following phases:

Phase 1: Development of Metrics and Test Plan

This phase included the necessary academic review of existing technical material for Crossbow integrated sensors and various IP cameras. Additionally, the research focused on the desirable attributes from the end-user's perspective. Measure of Performance and Measures of Effectiveness (MoP/MoE) were created. These were used to develop an effective test and evaluation plan.

Phase 2: Base-lining and Experimentation

Once a test and evaluation plan was created, the prototyped sensor-camera network was base-lined in the moderate operating environment of the Naval Postgraduate

School. The Crossbow Sensor suite has numerous data collection tools built-in. Additional tools such as network analyzers and packet sniffers were used. Following base-line experimentation, the system underwent the same procedures in various operating environments to include Point Sur and Thailand.

Phase 3: Analysis of Results and Conclusions

The final phase consisted of analyzing the results of each case study. The results were compared to the base-lined systems as well as the MoP/MoE's determined in Phase 1. By comparing the results from the case studies to the base-line test and the MoP/MoE's, one can determine the effectiveness and feasibility of deploying the system in real-world military and law enforcement environments.

E. THESIS ORGANIZATION

Chapter II of this thesis provides an overview of the technology behind wireless ad-hoc mesh networks and introduces the concept of wireless sensor networks. This chapter introduces sensor network architecture, layers, network components, and operating characteristics and constraints. Finally, this chapter introduces possible wireless sensor network applications.

Chapter III provides an overview of digital video technology. It introduces and briefly describes the topics of frame rate, video streaming, and compression. Additionally, it identifies the constraints and challenges of using cameras in real-world military and law enforcement applications.

Chapter IV describes the prototyped sensor-camera network. It introduces the COASTS 2006 research program and discusses the role of the integrated sensor-camera network in the operational scenarios. Additionally, Chapter V provides specific details of the selected network components.

Chapter V consists of the selection of metrics. It describes the characteristics of effective metrics. The chapter also describes the detailed test and evaluation plan used throughout the tests.

Chapter VI includes the results from the experimentations and case studies. Moreover, the results and implications of the tests are discussed. Performance characteristics illustrated by the various tests and operational scenarios are also discussed. Finally, Chapter VI provides several models intended to aid network architects in designing an integrated sensor-camera network.

Finally, Chapter VII surveys the entire study and addresses the conclusions reached concerning the feasibility and applicability of integrated sensor-camera networks for military and law enforcement applications. Additionally, Chapter VII discusses concerns and avenues for future research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. WIRELESS SENSOR NETWORKS

Although the concept of Wireless Sensor Networks (WSN) is an emerging field in computer science and information technology, the WSN relies on the well established technologies of wireless data networking and ad-hoc computer networks. A WSN consists of devices that combine the functionality of sensing, computation, and communication into a single, small form-factor device that is capable of self-organization and inter-device connectivity. Wireless sensor networks can potentially be used in a variety of military, law enforcement, and commercial applications. This chapter surveys the WSN, their characteristics, network architectures, and connectivity. Network protocols are discussed along with the challenges of security. In addition, power management, synchronization, and tracking are discussed. This chapter concludes with a brief overview of a variety of common sensors.

A. INTRODUCTION TO WIRELESS SENSOR NETWORKS

1. Development of Wireless Networks

As the term "wireless sensor network" indicates, a WSN is a subset of the wireless communications field. Wireless communications have been explored since the early twentieth century. The U.S. Army Signal Corps developed one of the first wireless paradigms in 1921 with the creation of the War Department Radio Net. By 1933, the War Department Radio net was a nationwide radiotelegraphic network that managed over a million words annually.

Even though the early days of wireless networks were relatively uncomplicated, they overcame many challenges and provided the framework for modern wireless communication networks. To overcome transmission range limitations, the early wireless networks used ad-hoc structures to transmit messages. The messages were transmitted along undedicated paths to any active relay station closer to the final destination. Additionally, the first Medium Access Control (MAC) protocols were developed by the

early wireless networks. Operators manually sent Request-To-Send/Clear-to-Send (RTS/CTS) messages. The National Traffic System first implemented standardized message formats and first introduced wireless multicasting.

Wireless communication continued to develop throughout the twentieth century. Limitations such as throughput, transmission power, and communications range have continually been addressed. Recently, wireless networks have become ubiquitous in private and commercial applications due to their inherent flexibility and low cost.

2. Ad-hoc Networks

An ad-hoc network is a self-configuring, peer-to-peer network with no defined infrastructure or topology. The redundancy and survivability of ad-hoc networks have made them especially appealing for military and commercial communication applications. The first successful ad-hoc data network was developed by the University of Hawaii in the early 1970s. The ALOHA NET, as it was called, was developed to provide data communications between the University of Hawaii and the outlying Hawaiian islands. It was a single-hop, packet-based, wireless network that used random-access protocols and MAC protocols.

In the early 1970s, the Defense Advanced Research Projects Agency sponsored an ad-hoc packet radio network known as PRNET. PRNET introduced many new concepts still used today. The first technology it introduced was the use of direct-sequence spread spectrum transmission. Additionally, PRNET introduced concepts in flow-control and error-control along with routing table update schemes. The Survivable Radio Network (SURAN) succeeded the PRNET. SURAN attempted to address many of the limitations of PRNET. It sought to increase the network capacity, to decrease node size and power requirements, and to increase security issues.

The interest of the academic research community exploded during the 1990s. The decreasing cost and size of hardware combined with the increase in computational abilities inspired several commercial, academic, and civilian uses of ad-hoc computer networks. In 1997, the Institute of Electrical and Electronic Engineers (IEEE) released the 802.11 standard, which includes basic ad-hoc networking capabilities.

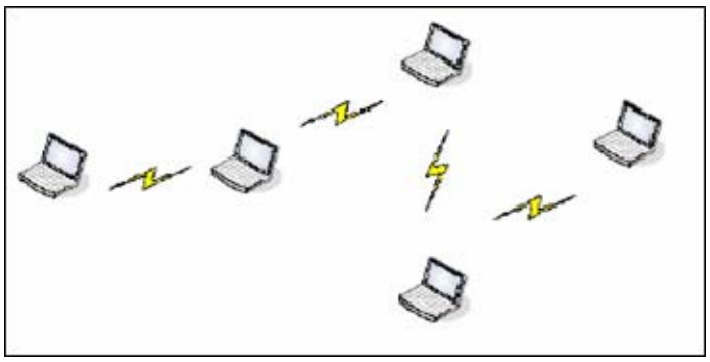


Figure 1. A Simple Ad-hoc Network

3. Characteristics of a Wireless Sensor Network

A wireless sensor network consists of devices that combine the ability to sense, compute, and communicate into a single small form-factor device. The WSN typically consists of distributed, low-power nodes, which are capable of self-organization and concurrent operations. Additionally, WSNs contain nodes with diverse sensing capabilities (Haenggi, 2005).

The ability to communicate between sensors provides the backbone of a wireless sensor network. The wireless sensor network inherits many of the communication attributes of wireless ad-hoc networks and combines them with the flexibility of mesh networks. The self-organizing abilities of a wireless sensor network are considered the most important communication feature. Their ability to organize themselves autonomously provides the capability for unattended, densely populated sensor grids for military and law enforcement use. Self-organization allows the sensors to identify and to communicate with other nodes in the surrounding area. A WSN does not require external coordination or administration to establish a network. Using dynamic routing protocols, the WSN can determine the most advantageous path to send information to its destination.

A second key characteristic in a WSN is the ability for the sensors to form a mesh network. A mesh network is defined as "a specific type of point-to-point connection in which there are at least two direct paths to every node … while a more restrictive definition requires each node to be connected directly to every other node" (Feibel, 1996). As a result, the WSN has a self-healing characteristic. That is, if one connection

or node is lost, the network will maintain functionality by simply re-routing the information along other connections. This is a vital characteristic because a WSN operates in adverse operating environments and is designed to have long on-station times.

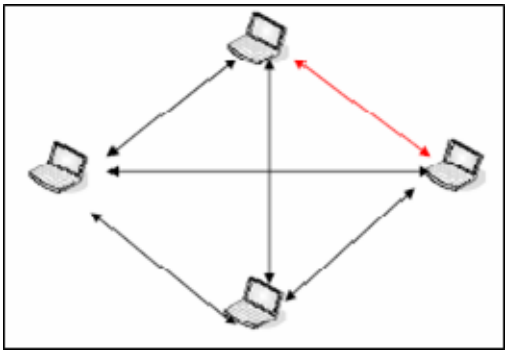


Figure 2. Mesh Network Topology

Wireless sensor networks employ a variety of sensing nodes. The number and type of sensors deployed vary depending on the intended purpose of the sensor network. For example, a sensor network used for intrusion detection might consist primarily of passive infrared sensors, magnetic sensors, and acoustic sensors while an environmental monitoring network will likely employ temperature, pressure, humidity and light sensors. Because the sensing capabilities do not affect the node's ability to communicate, a WSN can contain a wide variety of sensing types.

A wireless sensor network must be capable of performing numerous operations concurrently. Data gathering, which is essentially sensing data and disseminating the data, is the first fundamental operation a sensor must perform. The second fundamental operation is reporting. Report procedures consist of communicating data and the aggregation of the networks data. Sensor networks must be able to perform both functions simultaneously due to network distribution and limited storage capacity.

B. WIRELESS SENSOR NETWORK APPLICATIONS

The characteristics of sensor networks make them applicable to numerous environments. Because they interact deeply with the physical environment and can extend the reach of the existing Internet, sensor network applications are virtually

limitless. High-level tasks such as detection, classification, and tracking are common applications of sensor networks (Zhao & Guibas, 2004). The following overarching sensor network applications are based on the writing of Callaway (2004), Haenggi (2005), Culler and Hong (2004) and Culeer, Estin, and Strivastava (2004).

1. Industrial Control and Monitoring

Industrial factories, power plants, and production facilities are beginning to use wireless sensor network for controlling and monitoring systems. It is common to monitor the industrial complex for safety, maintenance and even quality control purposes. Traditionally, this process involves a complex and expensive wired network. However, as wireless sensor networks become more robust and reliable, they are quickly being applied to the industrial control and monitoring arena. The small size, self-forming and self-healing characteristics of WSNs make them appropriate for diverse applications ranging from balanced services, robots, assembly lines, and rotating equipment.

2. Environmental Monitoring

Wireless sensor networks are ideal for environmental applications due to their fault tolerance, self-organizing, and low power characteristics. Wireless sensor networks have applicability from climate control to water management to agriculture monitoring. Additionally, they can be configured to detect seismic activity, forest fires, floods, and even water quality. Environmental monitoring is, perhaps, the pioneering application for wireless sensor networks. Their innate characteristics meet the intense demands needed for proper environmental deployment.

3. Home Applications

A third emerging application for wireless sensor networks is home automation. Wireless sensor networks can be employed in a home environment similar to the ways they are deployed in environmental and industrial settings. Home automation provides increased control of home appliances and security. Climate control and security systems are the most common types of home automation applications. However, as technology

has increased, new applications are emerging. For example, refrigerators can be designed to monitor contents, determine what items need to be bought, and even provide customized temperature control depending on what items are in specific parts of the refrigerator. Currently, this is predominately achieved through installing traditional wired networks. WSNs provide the potential to increase the flexibility and sensing capabilities of home automation systems while simultaneously reducing costs by minimizing installation and maintenance costs.

Health monitoring is a second home application of wireless sensor networks. For example, networks can be used to monitor "body temperature, blood pressure, and pulse" of patients and to trigger some sort of alert or automated action depending on values (Haenggi, 2005). Additionally, sensor networks can be applied to toys. Their sensing capabilities and small size make WSN nodes perfect for designing toys of the future, which will act in complex manners.

4. Asset Tracking

Asset tracking is another key application for wireless sensor networks. This concept is applicable to both military and commercial organizations. Effective control and monitoring of supply chains can drastically increase the effectiveness of any organization. Many commercial companies have begun to employ radio frequency identifiers (RFIDs) to identify, to localize, and to track shipments. By placing wireless sensors inside shipping containers, efficiency can be increased by eliminating errors, streamlining the process, and increasing control of the supply chain (Callaway, 2004). With all aspects being equal, the organization with better control and awareness of its assets will be more efficient. For example, wireless sensors can be used to track critical objects through an organization's supply chain and to make changes to manage assets more effectively. This improved control of the supply chain makes just-in-time logistics a reality for high-tempo, dispersed organizations.

5. Military and Law Enforcement

Military and law enforcement applications are another promising field for wireless sensor networks. Joint Vision 2020 and Sea Power 21 advocate the use of unattended sensors for intelligent, surveillance, and reconnaissance. To best achieve these goals, a sensor network must be quickly deployable, have a long on-station time, and possess a variety of sensing capabilities. Wireless sensor networks are ideal for this type of application due to their self-organizing and self-healing characteristics. Since they have the high-level capabilities to detect, classify, and track objects, WSNs are ideal for physical security applications. For example, a WSN can be deployed around a perimeter to reduce the number of guards needed. They can be used as an early warning system to alert a quick reaction force. The diverse sensing capabilities of WSNs can also improve the command and control capabilities through battle-space monitoring (Haenggi, 2005). They can be used similarly to monitor equipment for the industrial applications. For example, WSNs can be used to monitor engine-room temperature and vibration levels on ships, aircraft and tanks. Additionally, they can be designed to detect chemical, biological, and nuclear attacks. They also provide the capabilities to develop "smart" weapons such as minefields, which discriminate between targets.

C. CONSTRAINTS AND CHALLENGES

Wireless sensor networks are a relatively new technology, yet they have many useful applications. The preceding section briefly introduced emerging applications in industrial monitoring, environmental monitoring, asset tracking, home applications, and military and law enforcement. As their capabilities increase, wireless sensors will become even more ubiquitous.

However, wireless sensors face numerous challenges in power management, localization, synchronization, security, and communication. For example, long on-station times combined with small form factor require nodes to use limited power sources efficiently. Localization refers to the node's ability to identify its physical location. Synchronization techniques are used to establish a network and to support localization. As with all wireless technologies, secure communications is paramount. Real-time communications are required for many sensor network applications.

1. Power Management

Most WSN applications require long on-station times. The small form factor associated with wireless sensors, however, results in limited power supply options. Traditional wired sensor networks can be powered over Ethernet or wall outlets, but wireless nodes must be powered by a self-contained power supply. Usually these power supplies are batteries or solar cells. As a result, power management is the most challenging constraint of wireless sensor networks. Power management can be divided into two categories: node-level management and system-level management.

a. Node-level Power Management

Node-level power management refers to the efficiency of the individual sensor nodes. A sensor node consists of four basic components. The first component is the microprocessor and memory unit, which is responsible for controlling the processing and logic tasks. The second component is the sensing unit, which contains the sensors that detect and interact with the environment. The third component is the communication unit, which consists of the radio circuitry for data transmission and reception. The final basic component of a node is the micro-operating system. This operating system is responsible for controlling the other components (Wang, Hassanein, & Xu, 2005). Node-power management begins with the design and selection of circuitry. Low-power chips and careful optimization of processes provide the foundation for energy efficiency (Holger & Willig, 2005). Dynamic power management is a technique often used to improve energy efficiency. This technique shuts down node components when they are not being used actively. Dynamic voltage scaling (DVS) is another technique to increase efficiency. DVS is the process of scaling supplied voltage to meet the instantaneous processor requirements (Raghunathan, Schurgers, Park and Srivastava, 2002).

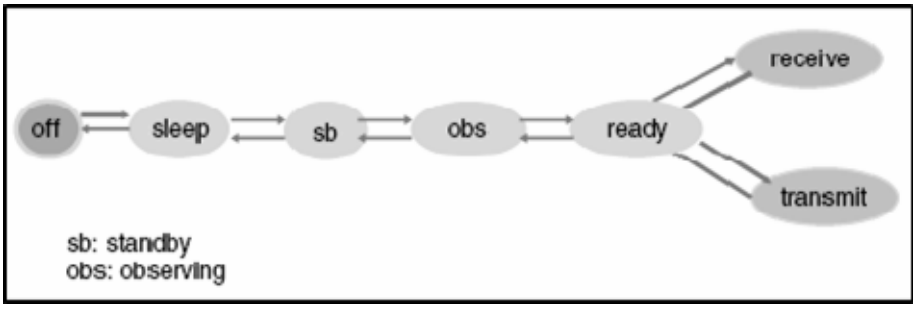


Figure 3. Node-level Power Management Diagram (From: Wang, Hassanein & Xu, 2005)

b. System-level Power Management

System-level power management involves controlling the transmission power of the sensor network as a whole. Controlling the transmission power affects many aspects of the sensor network. Communication ranges, battery life, network topology, routing paths, and transmission rates, for example, are aspects affected by transmission power (Wang, Hassanein, & Xu, 2005). The purpose of the sensor network often dictates the most efficient transmission power. An application that requires greater distances between nodes will require a greater transmission power, while a dense deployment scheme will require lower transmission power. System-level management also considers communication protocols and policies, such as rotating the nodes' functionality (Wang, Hassanein, & Xu, 2005). Many deployment strategies involve dividing the functionality of a node into sensing, computing, and data aggregation. Each function requires different amounts of energy. By rotating the functionality, one can extend the lifetime of the entire network.

Effective power management in a wireless sensor network is one of the most important and difficult challenges. At the node level, power management begins by properly designing the nodes. This often involves trade-offs between application requirements and technological capabilities. At the system level, power management involves the proper selection of the deployment scheme, transmission power, and architecture. By effectively managing power at the node and system level, one can produce WSNs with the extremely long lifetimes required by many applications.

2. Localization

Localization is the node's ability to determine its location. Localization can be divided into absolute localization and relative localization. Absolute localization relies on the use of Global Positioning System (GPS) satellites. Relative localization employs signal processing and determines a node's position with respect to the other nodes in the network. Using GPS receivers for localization is an attractive possibility; however, several factors make this less than ideal. GPS units tend to be large compared to the size of wireless nodes. They also require more power, which lowers the effective lifespan of a sensor node. Additionally, GPS units might not work well in congested areas, such as building or jungles (Murphy and Manoj, 2004). This section discusses many of the signal processing techniques researchers are investigating to achieve localization.

Achieving localization in indoor environments is significantly easier than outdoor environments. Indoor localization techniques commonly rely on fixed-beacon signals strategically placed throughout the area of operation. The sensor nodes receive the beacon signals and calculate the signal strength, angle of arrival, and time difference-of-arrival. These calculations allow the sensor to determine location through triangulation or some predetermined knowledge base (Sivalingam, 2002).

Outdoor deployment environments, on the other hand, increase localization difficulties. In such applications, there is no fixed infrastructure to pre-station beacons or calculate data used in a knowledge base. Outdoor sensor networks rely on GPS enabled nodes. Because GPS receivers consume relatively large amounts of power, only a few of the nodes are equipped with GPS and are often supplemented with extra power sources (Sivalingam, 2002). The non-GPS enable nodes will estimate position similarly to indoor networks. Signal strength is a good range estimator despite the sensitivity to the surrounding environment. Calculating the time difference-of-arrival and angle of arrival improves the accuracy of RF localization. A second localization algorithm assumes the beacon nodes broadcast location information to all nodes in the network and a central controller pivots the beacon signal at a continuous angular velocity (Nasipuri and Li, 2002).

3. Synchronization

As with traditional wired networks, synchronization refers to a common time reference. Synchronization supports network formation. It also supports localization by providing time difference-of-arrival capabilities. However, synchronization techniques in WSN are constrained by low-power characteristics.

Most wireless sensor networks use some sort of time division multiple access (TDMA) scheme to control communication flows. TDMA is used to sustain communications on wireless mesh networks. Additionally, synchronization is required to aggregate sensor readings effectively. Knowing when a sensor is reporting readings during the aggregation process is crucial. By accumulating the synchronized data, one can eliminate duplication, detect trends, track objects through a sensor grid, and present the end-user with a usable representation of the raw sensor data (Sivalingam, 2002).

Two categories of synchronization algorithms exist. The first category of synchronization algorithms achieves short-lived synchronization, known as pulsed synchronization. Pulsed synchronization relies on low-power broadcast beacons. The sensor nodes perform local synchronization by normalizing time stamps. Major drawbacks of pulsed synchronization schemes are the short duration of synchronization, the reliance on additional hardware, and the limited range associated with the need to be within transmission range of the beacon (Elson and Estrin, 2001).

The second category of synchronization algorithms achieves long-lasting global synchronization. Global synchronization protocols commonly rely on the knowledge of neighboring nodes' control signals and are common in cluster architectures. The node leader periodically transmits synchronization information to its neighbors, which then rebroadcast the information throughout the network (Ofek, 2002).

4. Communications

In order to achieve maximum applicability, sensor networks must support real-time communications. Real-time communications increase the end-user's knowledge and control of the surrounding environment. As a result, the time delay between sensing an event and communicating the event has emerged as a measure of WSN quality. Although

true real-time communication is difficult to achieve, several algorithms exist to minimize the delay between an event and to propagate the report to the base station efficiently. RAP and SPEED are two common protocols used to support real-time communications in WSNs.

The RAP protocol relies on the base station (BS) to coordinate queries. The BS contains the application layer of the sensor network, specifies the desired event information, and can query specific parts of the WSN to gather the desired information. The protocol ensures efficient communications by ensuring the arrival of queries to and from the addressed nodes. The SPEED protocol supports real-time communications by guaranteeing the maximum delay between communications. SPEED is a stateless architecture designed to create near real-time communications through congestion management and standardized delivery speed across the sensor network (He, Stankovic, Lu, and Abdelzaher).

5. Security

As with all wireless networks, network security is a challenge in implementing wireless sensor networks. Effective security provides the means of data authentication, data integrity, and privacy. Security issues are important to all WSN applications, but they are especially important in military and law enforcement applications due to the sensitive nature of the data. This section examines the security and privacy aspects of WSN and introduces several security protocols common in wireless sensor networks.

Wireless sensor networks have four characteristics, which impact network security (Slijepcevic, Wong, and Patkinjack, 2005). The first security related property of WSNs is the application's requirements and architecture. The inherent flexibility of WSNs allows the architect the freedom and capability to prioritize, adjust, and implement security measures. However, due to the computational and power restrictions of sensor networks, significant trade-offs exist between resources and achieved protection. Finally, the environments in which WSNs are deployed are often hostile.

D. WIRELESS SENSOR NETWORK ARCHITECTURES

The constraints and challenges associated with WSN node design combined with design and deployment objectives necessitate strict system architecture and topology. The low-power characteristic associated with WSNs greatly impacts the network architecture and topology due to the impact on networking and routing. Relatively, the power consumed by the node's sensing elements is far less than the power consumed by the data transmission elements (Wang, Hassanein, Xu, 2005). As a result, sensor network architectures must be structured to maximize efficiency and flexibility while being constrained by low transmission power and data rates. Wireless sensor network architectures can be classified in two general categories of "layered architecture" and "clustered architecture." As the following figure illustrates, these general categories can be further broken into sub-categories, such as negotiation-based, flat, query-based, hierarchical, and adaptive-based (Al-Kraki and Kamal, 2005). The general layered and clustered architectures are discussed in the following sections.

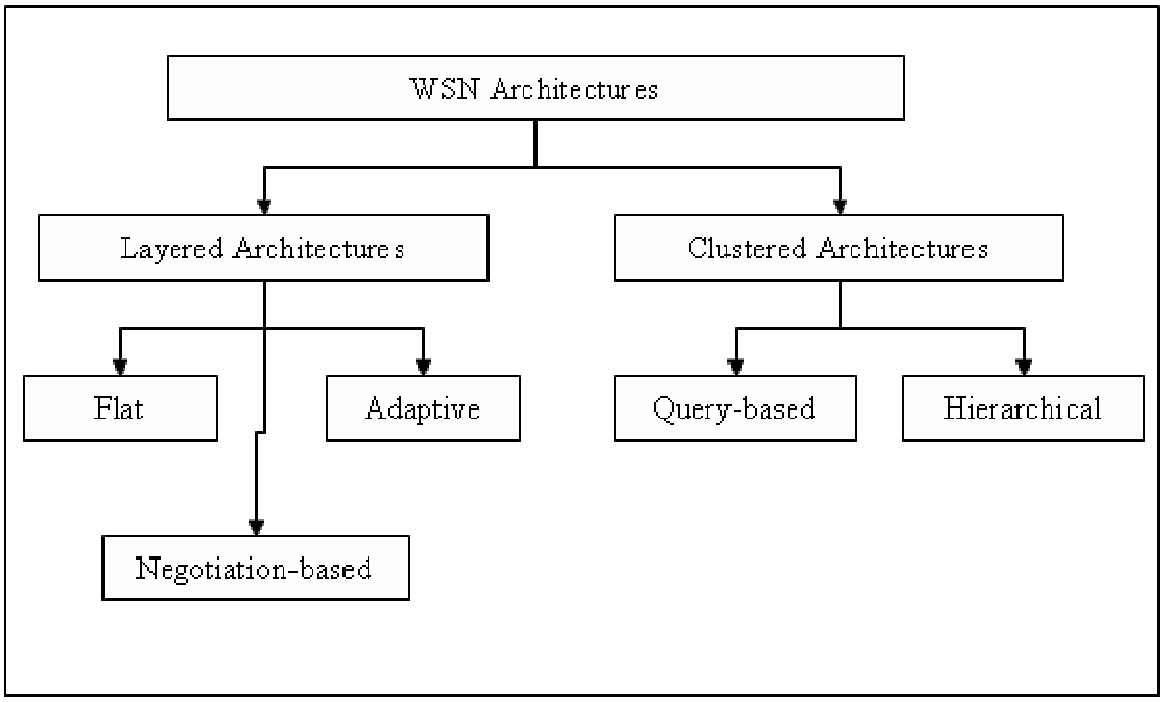


Figure 4. WSN Architectures (From: Woo et al., 2003)

1. Flat Network Architecture

In sensor networks using layered network architecture, a single base station (BS) and multiple node layers populate the network. Layers are formed by grouping nodes with an identical hop count to the base station. Figure 5 illustrates the layered architecture. The BS acts as a gateway or access point to a traditional wired network. Additionally, the BS collects and disseminates data gathered by the sensing nodes. The nodes create a wireless "backbone" for connectivity. End-users can access the network through a wired connection to the BS or through wireless transceivers such as Personal Digital Assitants (PDAs). The PDA can connect to the wireless backbone formed by the nodes. Flat network architectures are common in wireless sensor networks because they reduce the necessary transmission ranges and allow for more efficient use of power.

The Unified Network Protocol Framework (UNPF) is a set of protocols used to implement a layered architecture. The UNPF protocol relies on three operations to achieve a flat network: network initialization and maintenance, Medium Access Control (MAC), and routing protocols. During the network initialization phase, the BS will broadcast an identification beacon on the control channel. The nodes to which the BS can directly communicate form layer one. The layer-one nodes then transmit a second beacon signal. The nodes that receive beacon signals from layer-one nodes form layer two. This process is repeated until all nodes in the network are included in one of the network layers. After the network is established, the BS will periodically refresh the architecture by repeating the process (Murthy and Manoj, 2004).

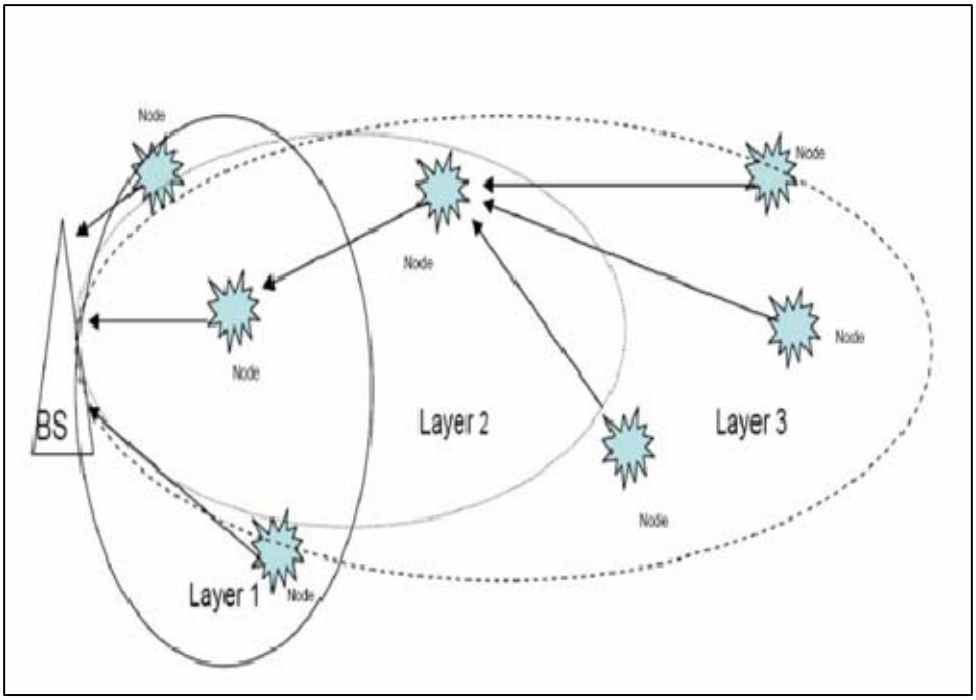


Figure 5. Layered Network Architecture (From: Murthy and Manoj, 2004)

2. Clustered Network Architecture

The second general wireless sensor network architecture is the clustered architecture, shown in Figure 6. Clustered architectures consist of a Personal Area Network (PAN) coordinator, or cluster head, which organizes the sensor nodes and communicates with the BS or external network. Clustered architectures are commonly used in situations in which data fusion is required. In these environments, the cluster head will gather the data from the sensor in the cluster and then transmit the data to the base station.

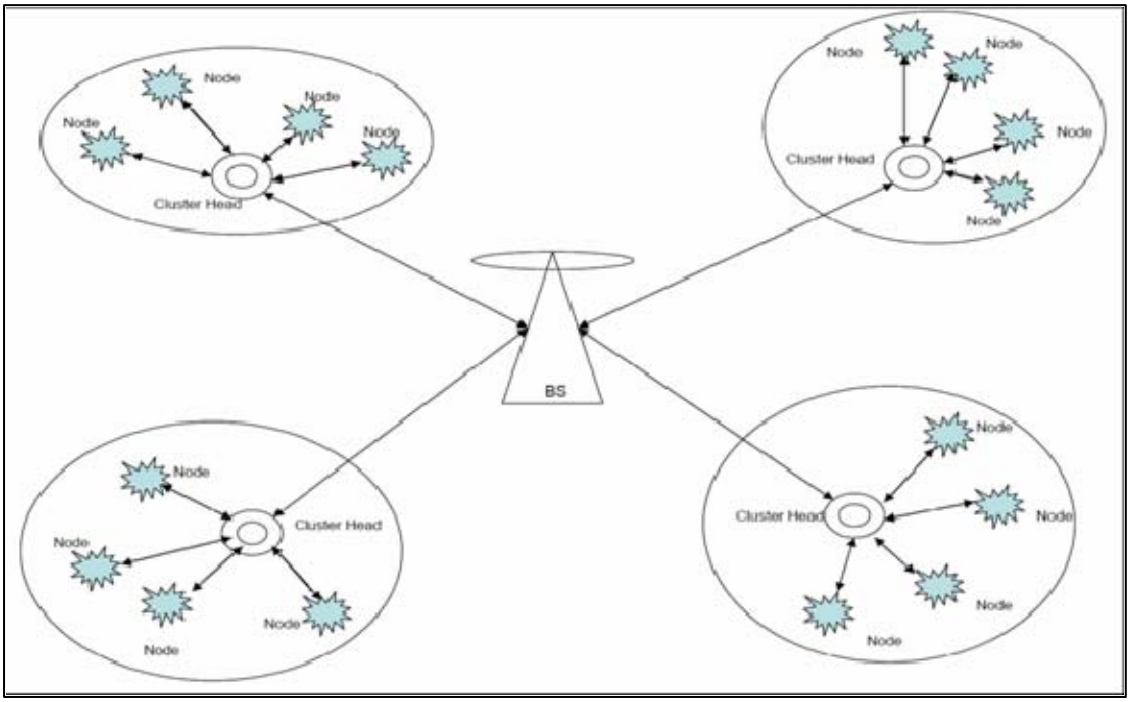


Figure 6. Clustered Network Architecture (From: Murthy and Manoj, 2004)

Clustered architectures rely on distributed network layer protocols, such as Low-Energy Adaptive Clustering Hierarchy (LEACH), to perform autonomous self-organization (Heinzelman, Chadrakasan, Balakrishman, 2000). The LEACH protocol consists of two main network stages: network set-up and steady state. In general, the network set-up phase is a relatively short, yet power-intensive process. To minimize energy consumption, LEACH randomly selects and changes the cluster head. By randomly selecting and periodically changing the cluster head, LEACH prevents one node from expending too much energy and helps to distribute the energy expenditures evenly. After being selected as a cluster head, the node will then broadcast its information to the other nearby nodes. The non-cluster head nodes then associate with the nearest cluster head by comparing the signal strengths received from the cluster heads. Once the network is formed, the cluster heads establish a TDMA communications schedule for all the nodes in that particular cluster. This marks the beginning of the steady-state phase of network operations. During this phase, the sensor nodes interact with the environment and communicate data to the cluster heads based on the TDMA

schedule. During this phase, LEACH attempts to conserve energy by processing and aggregating sensor data at the cluster-head level (Heinzelman et al., 2000).

This section described the two major classifications of sensor network architectures. The sub-categories were also introduced to the reader. The most common protocols for network formation were discussed. This section also detailed how the characteristics of self-organization and low-power constraints govern wireless sensor network architectures. The following section discusses the typical protocols found in WSNs.

E. WIRELESS SENSOR NETWORK PROTOCOLS

As with all other computer networking environments, WSNs use a layered protocol similar to the OSI 7 layer stack. The general layered protocol stack for wireless sensor networks is illustrated in Figure 7 below. The application layer is responsible for analog-to-digital conversion. The network layer handles the seamless transfer of information while the data link layer handles fair access and error control. The physical layer allows the data stream to be transferred and received.

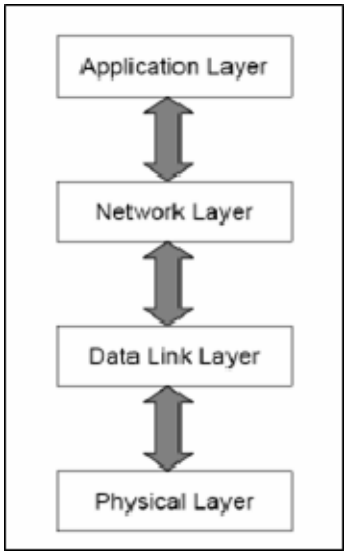


Figure 7. Typical Protocol Stack (From: Stallings, 1996)

In the following sections, the layer's roles are discussed in further depth.

1. Physical Layer

Due to the inherent power constraints, wireless sensor networks are designed to use low-bit rates during transmission. Low-bit rates reduce the needed transmission power and, therefore, support long battery life and aid in self-organization. Although sensor networks can use infrared communications, radio frequencies (RF) are the most common and are the focus of this section. Several RF techniques are commonly found in WSNs, including PiccoRadio, Wireless Integrated Network Sensors (WINS), and the 802.15 Standard for Wireless Personal Area Networks (WPAN). PiccoRadio techniques rely on the use of ultrawide band communications (Rabaey, Ammer, Silva, Patel, and Roundy, 2000). Like 802.11, WINS uses spread-spectrum techniques in the unlicensed Industrial, Scientific, and Medical (ISM) frequency ranges (Callaway, 2004).

Many commercially available sensor systems use the recently adopted 802.15 family of standards. The 802.15 family supports three different physical layer methods. The first standard, 802.15.1, uses Bluetooth technology as the basis for transmission. The 802.15.3 standard is the high-bit-rate WPAN protocol. The final, and perhaps most common, is the 802.15.4 protocol, which is a low-bit-rate, spread-spectrum technique.

2. Data Link Layer

The data link layer has two roles: to provide fair access to the physical layer and to provide error control during transmission. The nature of the data gathered by sensor nodes and the time sensitive qualities make fair access to the transmission layer and error-free transmission extremely important wireless sensor networks.

This section briefly discusses challenges and categories associated with MAC protocols. Additionally, it provides a brief description of commonly used MAC protocols.

The MAC protocol serves as an intermediary between the physical layer and the upper layers of the protocol stack. Traditionally, the MAC layer coordinates and interfaces with the network layer by using logical link control. The MAC protocol

typically supports the physical layer by using the most efficient data frame size and frequency of transmission. As a result, the MAC protocol affects energy management, synchronization, timing, flow control and error control.

MAC protocols employed by WSNs can be categorized in to three types: fixed-allocation, contention-based, and demand-based. Fixed-allocation protocols provide fair access to the transmission medium by following a predetermined transmission schedule. As a result, fixed-allocation protocols are best suited for sensor networks where the traffic is predictable, such as environmental monitoring. Contention-based protocols are often used in sensor networks where there is non-deterministic traffic. However, contention-based protocols often result in traffic collisions that cause delays of time-sensitive data. Demand-based protocols are a time-varying technique that allocates channel usage based on node demand. Demand-based protocols are well suited for variable rate traffic despite the overhead associated with reserving the transmission channel (Murthy and Manoj, 2004).

There are four common MAC protocols in these categories: Self Organizing MAC for Sensor Networks (SMACS), Eavesdrop and Register (EAR), Hybrid TDMA/FDMA, and CSMA-Based.

SMACS and EAR compliment each other to handle mobility and network initialization. SMACS handles network initialization through link-layer associations. It also handles the node discovery process and the channel assignment process concurrently. A communication link is established consisting of a pair of time slots operating at a randomly chosen, but fixed frequency. SMACS achieves power conservation by using random wake-up schedules during the connection phase and disabling the radio during idle time slots. The EAR algorithm is used to ensure a seamless connection between nodes even if a node is mobile. The EAR algorithm uses specific mobile nodes to update neighbors and to terminate poor connections (Sohrabi, Gao, Ailawadhi, and Pottie, 2002).

The Hybrid TDMA/FDMA protocol is a centrally controlled MAC scheme. It uses sensors with energy limitations designed to communicate directly to a single, nearby BS. By using a hybrid TDMA/FDMA protocol, the network achieves effective time

synchronization while minimizing the bandwidth required for operations. The TDMA aspect of the protocol is used to reduce delays that affect synchronization. The FDMA scheme allows the minimum signal bandwidth per node. The hybrid MAC scheme uses an ideal number of channels to diminish the power expended during set up and communications. This number is determined by a ratio of the transmitter power to the receiver power. If the receiver power expenditure is greater, the hybrid scheme is more FDMA oriented. However, if the transmitter power is greater, it tends to be TDMA oriented, due to the ability to disable the radio during idle periods (Shih, Cho, Ickes, Min, Sinha, Wang and Chandrakasan, 2001).

CSMA-based MAC schemes are generally best suited for networks generating random traffic flows. As with traditional computer networks, the CSMA-based MAC algorithms are contention-based—that is, they are designed to handle the possibility of collisions. CSMA-based MAC schemes use binary exponential back-off techniques to reduce the likelihood of multiple collisions. They also control data rates so that nodes close to the BS do not dominate over those further away from the BS (Woo and Culler, 2001).

3. Network Layer

As with wired networks, the WSN network layer is responsible for controlling network operations, such as routing packets through the network. The distributed, ad-hoc nature of WSNs makes routing data difficult. This difficulty is only compounded by the low transmission power associated with the networks. Routing protocols control how data flows from the source to the destination. As a result, protocols greatly affect the efficiency of the network. Several routing techniques are commonly used in sensor networks and are briefly discussed in the following sections.

a. Routing Techniques for Layered Architectures

Flooding, gossiping, and rumor routing are the most common routing techniques used in layered sensor network architectures. The first and most uncomplicated routing technique is called “flooding.” Flooding is when the data packet is continually rebroadcast until the final destination is reached or until a maximum hop

count is reached. Even though this technique avoids complexity, it causes data duplication, network congestion, and is not energy efficient. Gossiping is a modified version of flooding. In the gossiping technique, the data are not broadcast, but rather transmitted to a randomly selected neighbor. Gossiping prevents data duplication but does not provide the needed reliability. Rumor routing is designed for best effort delivery. It does not produce the optimal routing; however, it does reduce data duplication and network traffic. The disadvantages of rumor routing are that the routing parameters depend heavily on the topology and that the delivery of data is not guaranteed (Braginsky and Estrin, 2002).

b. Routing Techniques for Clustered Architectures

Cluster-based architectures require more evolved routing techniques. The layered architecture routing techniques work well when the primary communications are with the BS. However, in clustered architectures, routing between the clusters is difficult. One common protocol is the Directed Diffusion. Directed Diffusion allows the destination to specify the data-rate requirement based on the ability to report on the destination's interests (Intanagonwiwat, Govindan and Estrin, 2000).

Peer-to-peer enabled architectures are a subset of clustered architectures. Peer enabled routing techniques include Cost-Field approach, Geographic Hash Table (GHT), and Sensor Protocols for Information via Negotiation (SPIN). Cost-Field algorithms attempt to find the optimal path by calculating the cost, or number of hops. When data packets are sent, the "cost-so-far" field is updated as the packet transverses the network. As the algorithm continues, the system is able to find the path of least-cost to various destinations (Ye, Chen, Lu, Zhang, 2001). The GHT compiles geographic coordinates and identifies which nodes are in the different geographic areas. When a sensor wants to pass data to a node not in its own geographic area, it will pass the data packet to the nearest node in the same geographic area as the destination node (Tatnasamy, Karp, Yin, Yu, Estrin, Govindan, Shenker, 2002). The SPIN algorithm is similar to flooding, but overcomes the weaknesses through negotiation and resource

versatility. Negotiation reduces data duplication by dynamically determining the optimal path. This, in return, helps minimize errors and prolongs network lifetime (Perrig, Szewcyzk, Wen, Culler, Tygar, 2001).

The power constraints associated with sensor networks have resulted in the creation of many routing protocols that consider efficiencies at multiple levels in the protocol stack. One such protocol is LEACH, discussed previously. XMesh is another such protocol. XMesh was derived from the Surge-Reliable and Mint Route protocols developed by Hill and Woo. XMesh is a commonly used protocol that can provide the self-organizing, low-power, self-healing attributes required by WSNs. XMesh employs idle periods and transmission periods. The protocol "awakens" the idle node eight times per second for transmission. When a node wakes up, it first determines if another sensor is transmitting. If another sensor is transmitting, it prepares to receive data. If no other node is transmitting, it can either send its own data or retransmit data received from another node. XMesh uses messaging to establish the best route and also uses dynamic voltage scaling to minimize the number of hops.

4. Application Layer

The application layer of sensor networks is the sensors themselves. The role of the sensor is to interact with the environment, detect a physical phenomenon, and to convert it into transmittable data. Once the data are packetized, they are sent to the appropriate node or BS for further operations.

F. IEEE 802.15.4 PROTOCOL

The IEEE 802.15.4 protocol was approved in 2003, specifically to support networks requiring low data rates and low transmission powers. The 802.15 family is well suited for low data rate applications; however, the other family members do not support low-power transmissions needed for sensor networks. As a result, the standard has been adopted by many commercially available sensor networks. For example, many

home automation and security applications use the IEEE 802.15.4 standard because they require low-to-medium bitrates, and moderate amounts of delay are acceptable (Holger and Willig, 2005).

The IEEE 802.15.4 standard describes two types of devices on a Low Rate WPAN (LR-WPAN). The standard supports full-function devices (FFD) and reduced-function devices (RFD). RFDs are used in simple applications with minimal amounts of data traffic. RFDs typically only communicate with a specific FFD. FFDs are used in more complex environments with high data traffic.

The LR-WPAN is based on the Open System Interconnection (OSI) seven-layer model illustrated in Figure 8. However, the application and network layers are not addressed by the IEEE 802.15.4 standard. Only the physical layer and the MAC layer are included in the standard. The standard relies on the Type I 802.2 Logical Link Control (LLC) and the Service Specific Convergence Sublayer (SSCS) to interact between the lower levels and the upper levels (IEEE 802.15.4 Standard, 2003).

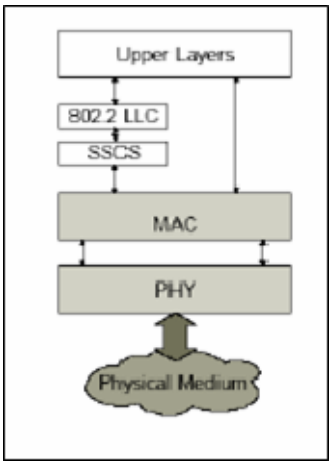


Figure 8. Open System Interconnection (OSI) Seven-Layer Model (From: IEEE 802.15.4 Standard, 2003)

1. Network Formation

The most appropriate topology for a sensor network depends largely upon the application. The standard allows the LR-WPAN to operate in a star or peer-to-peer topology. The following sections detail the network formation processes associated with the various topologies.

a. Star Network Topology

In the star topology, a single PAN coordinator governs the communications between sensor nodes. The PAN coordinator is typically a FFD, which initiates and terminates the network communications throughout the network. As Figure 9 (a) shows, the PAN coordinator also handles the routing between the network nodes. The coordinator assigns a unique identification to all members in its sphere of influence and broadcasts its own identification. Nodes associate with the coordinator by responding to the broadcast. If a node is within range of two coordinators, it will respond to only one broadcast (IEEE 802.15.4, 2003).

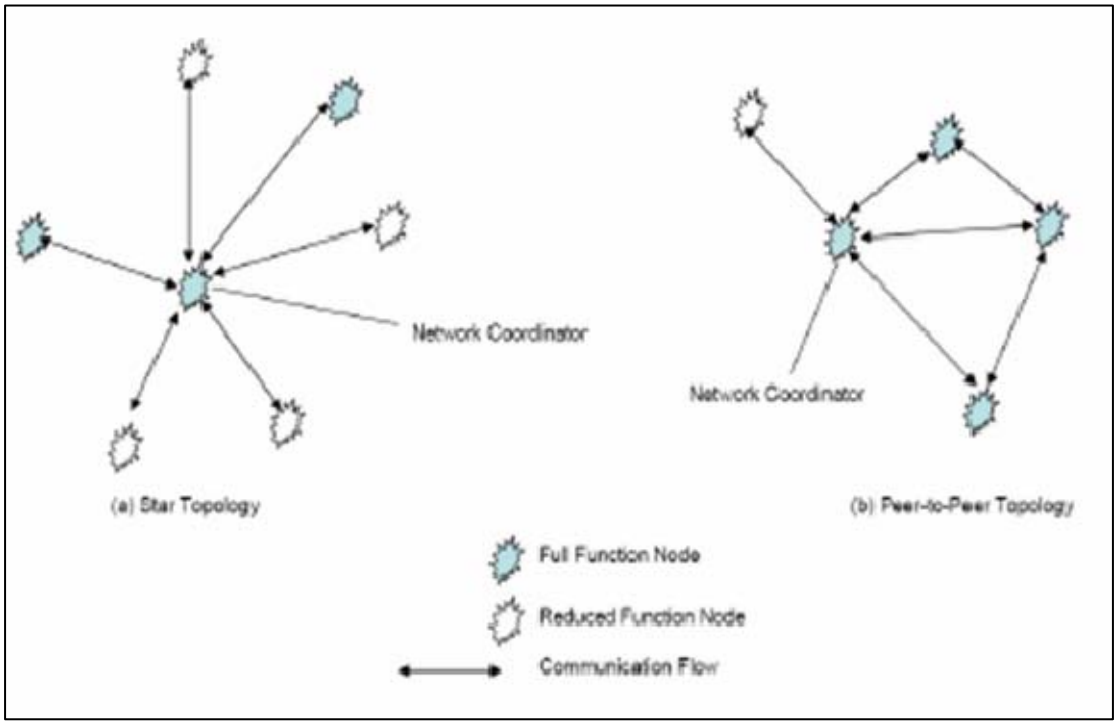


Figure 9. Star and Peer-to-Peer Topologies (From: IEEE 802.15.4 Standard, 2003)

b. Peer-to-Peer and Cluster Formation

The peer-to-peer topology, shown in Figure 9 (b), consists of a network coordinator, which coordinates with the other FFD and RFD nodes. The peer-to-peer topology is distinct from star topology in that the nodes can communicate among themselves.

The peer-to-peer topology supports the networking characteristics desirable in a sensor network. Peer-to-peer networking allows the formation of truly ad-hoc, mesh, multi-hop, self-healing networks. Like the star topology, the peer-to-peer topology also consists of a network coordinator. Even though the nodes can communicate among each other, they associate with only one PAN coordinator. Through the use of the PAN identification and the node identification, communication between PANs becomes possible. This results in the formation of clusters. Clusters are comprised predominately of fully functional nodes. A RDF can be part of a cluster, but it is restricted to only communicating with the coordinator. The PAN coordinator provides synchronization for other devices. The first PAN coordinator establishes itself as the cluster head (CH) and has a cluster identifier (CID) of zero. The CH then broadcasts this information. Nodes that receive the broadcast associate with that cluster. If a node does not receive the beacon but can communicate with other nodes, it will form a new cluster. This process is repeated until all the nodes are associated with a cluster. Cluster formation is depicted in Figure 10.

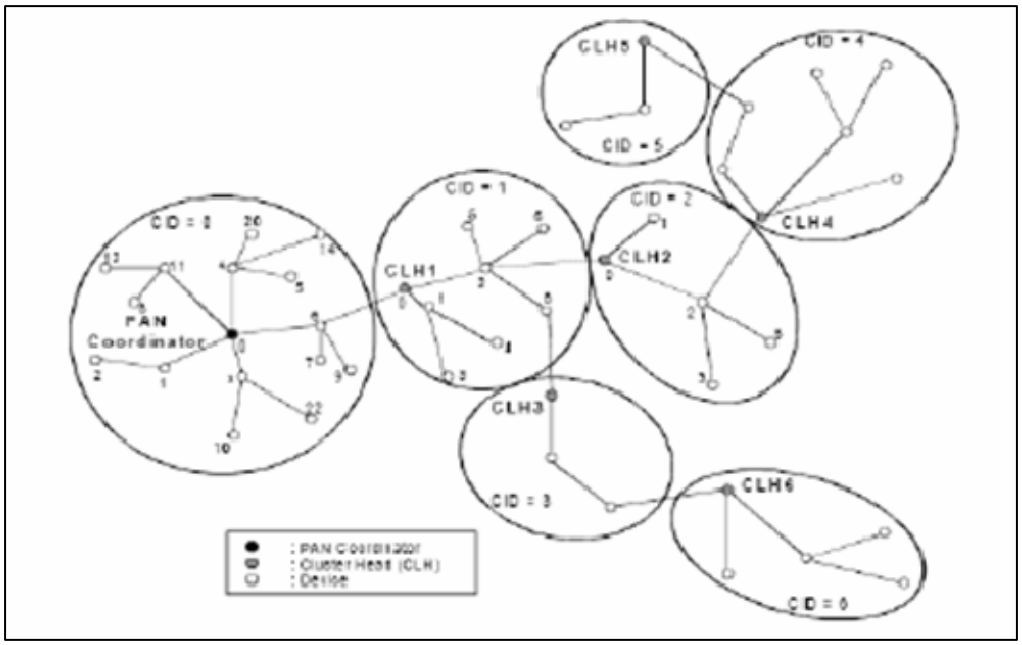


Figure 10. Cluster Formation Using Peer-to-Peer Topology (From: IEEE 802.15.4 Standard, 2003)

2. Physical Layer

The first layer described by the 802.15.4 standard is the physical (PHY) layer. The standard identifies two primary PHY layer services. The PHY data service is responsible for controlling the radio and the transmission and reception of the data units. The second service, management services, performs Energy Detection (ED), Clear Channel Assessment (CCA) and Link Quality Indication (LQI) for the network. The standard also provides specification for turn-around-time, transmission power, LQI, and CCA for all of the approved frequency bands. Turn-around-time is the period between the ability to transmit and the ability to receive, or receive-to-transmit. The 802.15.4 standard requires a twelve-symbol turn-around-time. Moreover, the standard mandates that transmitters be designed to operate with at least -3dBm and have the ability for low-power transmission to minimize interference. The maximum transmission power is regulated by the Federal Communications Commission (FCC). The PHY provides three manners to conduct CCA: detecting energy above a defined threshold, carrier sense only, and carrier sense with energy above a threshold. The carrier-sense method indicates a busy channel when a signal is detected that matches the IEEE 802.15.4 modulation and spreading standards (IEEE 802.15.4 Standard, 2003).

The physical layer of the 802.15.4 standard specifies three frequency frequencies. The 868-868.6 MHz frequency range is predominately used in Europe. The 902-928 frequency range is used predominately in North America. The 2400-2483.5 MHz range is approved for world-wide use. All of the approved frequencies fall within the unlicensed ISM band. The PHY layer uses Direct-Sequence Spread Spectrum (DSSS) techniques. The different frequency ranges use different bit rates and numbers of channels. Additionally, they use either Binary Phase Shift Keying (BPSK) or Quadrature Phase Shift Keying (QPSK) as the modulation technique. The following table summarizes the physical layer options supported by the 802.15.4 standard.

PHY (MHz)	Frequency Band	Modulation	Bit Rate	Number of Channels
868/915	868-868.6	BPSK	20	1
	902-928	BPSK	40	10
2450	2400-2483.5	O-QPSK	250	16

Table 1. Frequency Bands and Data Rates for IEEE 802.15.4 (From: IEEE 802.15.4 Standard (2003))

3. Medium Access Control Layer

The MAC layer serves as the interface between the SSCS and the physical layer. The MAC layer provides two key services for the protocol. The first service is the MAC data service. The MAC data service is responsible for ensuring successful transmission and reception of the data units (illustrated in Figure 11), through the PHY data service. The MAC management service acts like the device coordinator. It is responsible for managing the beacon signals, PAN association or disassociation, error control and validation, and for maintaining reliable links between nodes. Additionally, the MAC management service provides device security. Finally, the management service implements a CSMA-CA process to ensure channel access and to avoid data collisions.

The IEEE 802.15.4 standard identifies four acceptable frame types: the beacon frame, data frame, acknowledgement frame, and the MAC command frame. The frame formats are based on the general MAC frame format shown in Figure 11. The MAC Header (MHR) consists of the frame control, sequence number, information field, and the

MAC payload. The Frame Control field identifies which frame type it is. The sequence number identifies where the frame falls in the sequence of frames sent. The final parts of the frame are the MAC Footer (MFR) and the Frame Check Sequence (FCS).

<table>
<tr><th>Octets: 2</th><th>1</th><th>0/2</th><th>0/2/8</th><th>0/2</th><th>0/2/8</th><th>Variable</th><th>2</th></tr>
<tr><td rowspan="2">Frame Control</td><td rowspan="2">Sequence Number</td><td>Destination PAN Identifier</td><td>Destination Address</td><td>Source PAN Identifier</td><td>Source Address</td><td rowspan="2">Frame Payload</td><td rowspan="2">FCS</td></tr>
<tr><td colspan="4">Addressing Fields</td></tr>
<tr><td colspan="6">MHR</td><td></td><td></td></tr>
</table>

Figure 11. General MAC Frame Format (From: IEEE 802.15.4 Standard, 2003)

The following figures illustrate the four MAC frame types. The beacon frame is sent periodically by the PAN coordinator. The beacon is used to provide information about the network management and to provide synchronization of the network devices. The data frame is used to transmit data received from the higher layers. Like traditional wired networks, the data are encapsulated into the data frame. If the data being sent exceed the data payload size, they are broken into multiple data frames. It is important to note that when a node receives a data frame from another node, it is not required to send an acknowledgment frame. The acknowledgement frame is used to confirm receipt of a transmitted frame. The final frame is the command frame. This frame is used to communicate actions between the nodes, such as association, disassociation and beacon requests.

<table>
<tr><th>Octets: 2</th><th>1</th><th>4/10</th><th>2</th><th>Variable</th><th>Variable</th><th>Variable</th><th>2</th></tr>
<tr><td>Frame Control</td><td>Sequencing Number</td><td>Addressing Fields</td><td>Superframe Specification</td><td>GTS Fields</td><td>Pending Address Fields</td><td>Beacon Payload</td><td>FCS</td></tr>
<tr><td colspan="3">MHR</td><td colspan="4">MAC Payload</td><td>MFR</td></tr>
</table>

Figure 12. Beacon Frame Format (From: IEEE 802.15.4 Standard, 2003)

Octets	1	(see 7.2.2.2.1)	Variable	2
Frame Control	Sequence Number	Addressing Fields	Data Payload	FCS
MHR			MAC Payload	MFR

Figure 13. Data Frame Format (From: IEEE 802.15.4 Standard, 2003)

Octets:2	1	2
Frame Control	Sequence Number	FCS
MHR		MFR

Figure 14. Acknowledgment Frame Format (From: IEEE 802.15.4 Standard, 2003)

Octets: 2	1	(see 7.2.2.4.1)	1	Variable	2
Frame Control	Sequence Number	Addressing Fields	Command Frame Identifier	Command Payload	FCS
MHR			MAC Payload		MFR

Figure 15. Command Frame Format (From: IEEE 802.15.4 Standard, 2003)

G. ZIGBEE

The ZigBee standard is a rapidly growing standard developed by a non-profit industry consortium designed to produce "a reliable, cost-effective, low-power" open global standard (Heily, 2004). As Figure 16, shows ZigBee is designed for low throughput and short-range networks.

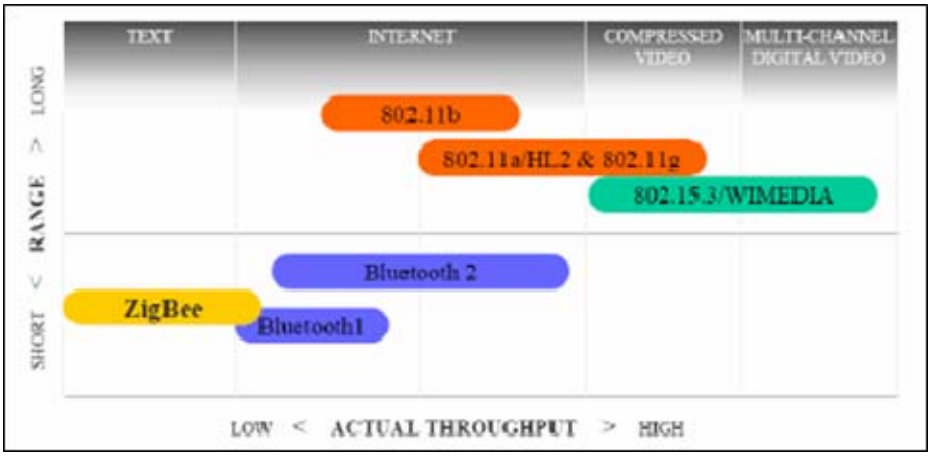


Figure 16. Overview of Wireless Communication Standards (From: Heily, 2004)

The ZigBee standard is not intended to replace the IEEE 802.15.4 standard. Instead, it is designed to expand upon the existing 802.15 infrastructure. The ZigBee framework builds upon the network and application layers of the protocol stack (Craig, 2005). The ZigBee standard further identifies possible network topologies, including star, mesh, and cluster tree. It allows for larger networks by increasing the local addressing to 16-bits. The ZigBee network layer has responsibilities similar to the 802.15.4 standard but is expanded to include the establishment of the network, new device configuration, addressing assignment, synchronization, security and routing (Kinney, 2005).

At the physical layer, ZigBee further expands upon the concept of Full Function Devices and Reduced Function Devices. ZigBee introduces the concept of "logical devices" to sensor networks. It relies predominately on FFDs but allows the use of RFDs. The first logical device is the "ZigBee Coordinator." The ZigBee Coordinator is similar to a BS or CH. The coordinator is responsible for initializing and maintaining the network. Under the ZigBee Coordinator is the "ZigBee Router." The router is responsible for routing traffic throughout the network. In accordance with the 802.15.4 standard, these two devices must be FFDs. The final device introduced is the "ZigBee End Device." The end device is the lowest level of the network. These devices are solely responsible for interacting with the environment and forwarding detection information. They may be FFDs or RFDs because they only communicate with higher level devices. Figure 17 illustrates the various topologies and node type introduced by the ZigBee standard.

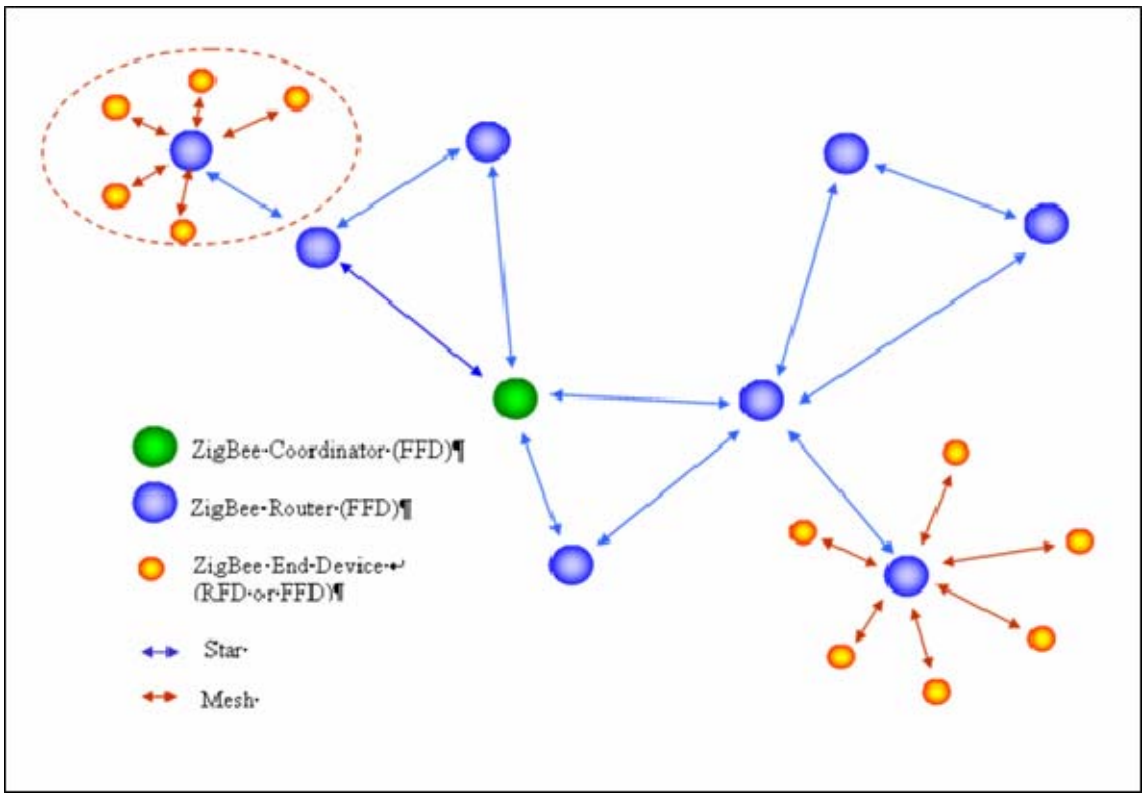


Figure 17. ZigBee Network Topologies and Node Devices (From: Kinney, 2005)

The ZigBee standard also addresses the issue of security in WSNs. ZigBee adds security to the MAC layer through the use of encryption. It adds a header to the MAC frame, which indicates if a frame is encrypted. For encryption at the MAC layer, the ZigBee standard uses either the Counter mode of AES or the Cipher Block Chaining mode. In addition, frame integrity is checked using the Message Integrity Code (MIC). At the network layer, ZigBee relies on a modified combination of Counter mode AES and Cipher Block Chaining mode. The network layer is responsible for encrypting the information it adds to the data frame. At the application layer, ZigBee behaves similarly to the lower levels. It uses a key to secure the message and then encapsulates it into a data frame.

The ZigBee specifications expand upon the IEEE 802.15.4 standard and move toward a universally accepted standardization for wireless sensor networks. ZigBee adds the support for the traditional OSI 7 layer model. Furthermore, it increases the security

capabilities, which are important, due to the sensitive nature of WSN data. The ZigBee protocol is quickly being adopted by commercially available sensor networks.

This chapter introduced wireless sensor networks and described key WSN areas. The early evolution of WSNs from wireless and ad-hoc mesh networks was discussed. This chapter also discussed the variety of WSN applications and the challenges associated with each application. Then, the constraints and challenges that are unique to wireless sensor networks were discussed. Next, this chapter introduced the major WSN architectures and the advantages and disadvantages with each. Wireless Sensor Network protocols were also examined in detail. Additionally, the IEEE 802.15.4 protocol was presented. Finally, this chapter described the new ZigBee protocol designed for world-wide acceptance. This chapter provided the technical and theoretical background of sensor hardware, network design, and experiments covered in future chapters.

III. VIDEO TECHNOLOGY

Video imaging technology has been actively used since the early twentieth century. Video technologies are used in numerous applications, including providing information, entertainment, and historical documentation. Today, video imaging is used in countless military and law enforcement applications. Understanding the processes that provide video from a remote sensor to the watch-stander is an important part of network design. This chapter introduces key concepts of video image capturing, encoding, and delivery.

A. DIGITAL VIDEO AND IMAGING INTRODUCTION

Digital imaging devices rely on traditional camera optics combined with silicon charge-coupled device (CCD) chips. CCDs focus and convert the reflected light into electronic signals. They are clusters of light receptors that convert the received light into three discrete electrical signals. The electrical signals are then converted to digital information through the digitization process.

Digitization converts the electrical signals into digital information through sampling and quantization. Sampling is the measurement of electrical energy created by the CCD within a specific region or time period. Quantization is the process of assigning an integer value to represent the amplitude of the electrical energy sampled. The sampling and quantization processes are repeated until an entire digital representation of the physical image is created. The accuracy of a digital representation of real or analog information is related directly to sampling and quantization. Increasing the sampling rate produces more discrete digital samples of the same analog signal. This allows for a more accurate representation of the image signal. Increasing the number of quantization bits allows the accurate representation of the amplitude of the image signal. For example, an image signal represented by only two quantization bits is less accurate than the same signal with ten quantization bits. The combination of sampling rates and quantization allow digital images to represent the real image accurately.

The digital representation of the image is presented as a matrix of values. Each value represents the color and intensity of a specific area of the image. The specific element is known as a picture element, or pixel. The digital video image is achieved through the aggregation of hundreds or thousands of pixels. The final digital image can then be transmitted, displayed, or stored in various manners. Digital video is increasingly being transmitted using the Transmission Control Protocol/Internet Protocol (TCP/IP) but is also transmitted using radio frequencies.

The number of pixels on the CCD chip determines the quality of the digital image. Additionally, the number of lines and the number of pixels per line determine the quality of the image. As the number of pixels rises, each pixel represents a smaller part of the image, thus allowing for more detail to be shown. Several standard image formats have been designed to specify resolutions and aspect ratios commonly used to display digital images. Table 2 summarizes resolutions for the standard image formats.

	Sub-QCIF	QCIF	CIF	4CIF	16CIF
Width in Pixels	128	176	352	704	1408
Height in Pixels	96	144	288	576	1152

Table 2. Image Format Resolutions (From: Wang, 2002)

Digital video technology covers the capturing, storing, and displaying a series of images captured. An additional item of interest is the image refresh rate, or frame refresh rate. The frame refresh rate determines temporal resolution. Temporal resolution is a trait of digital video that refers to the representation of motion during a given time. Most forms of video simulate motion by displaying still picture frames at a high rate. Slight differences in the frames are observed as motion. Frame rates for digital video are commonly between 15 and 60 frames per second. Temporal resolution significantly improves with higher frame refresh rates (Poynton, 1996).

B. DATA RATE CONSIDERATIONS

Digital video images require robust communication channels due to the relatively large data rates required for accurate video. Each pixel of the CCH chip contains a detector for each of the three primary colors of light. The light detected is converted to luminance and chrominance values, which represent intensity, hue, and color saturation. Each detector commonly uses eight bits to represent these values, resulting in 24-bits per pixel needed to send a single frame of uncompressed video. Assuming the video is transmitting at 4cif, or 704 x 576, each frame requires 405,504 pixels. At 24-bits per pixel, each frame requires 9,732,096 bits.

In addition, the temporal resolution must be high to provide near-streaming video. For digital video surveillance in a tactical or security application, it is not necessary to have flicker-free video. Assuming a steady, but modest, 15 frames per second, the video would require 145,981,440-bits.

Standard wireless networks can pass between 11- and 54-Mbps of throughput to each client on the network. Given a network passing 25-Mbps, digital video must be compressed six times to pass the video stream over the network. Even at this level of compression, a single network client viewing the video would consume the entire network throughput. However, several compression techniques have been developed to allow the efficient transmission of digital video. The following section describes the most common compression techniques used for digital video.

C. DIGITAL IMAGING COMPRESSION

The considerable data rate requirements for digital video demonstrate the need for effective compression techniques to allow digital video to be efficiently passed over networks. Compression algorithms take advantage of statistical and psychological redundancies found in digital images. Two common open compression techniques, JPEG and MPEG, are discussed below.

1. JPEG and Motion JPEG

A working group under the ISO, the Joint Pictographic Experts Group, developed a general purpose still-image compression standard. The standard, known as JPEG, is intended to address transmission and storage problems. The JPEG standard effectively compresses grayscale and color images, but does not compress black and white images with sudden jumps in color well due to spatial predictive coding used.

The JPEG standard was formally adopted in 1995 by the ISO. Although there is no noticeable degradation to image quality, JPEG is considered a lossy compression because the algorithm discards original data that are imperceptible to the human eye. Motion JPEG, or MJPEG, is often used in digital video applications. Using the Motion JPEG, each frame is compressed into a JPEG image. This approach produces high quality video at high resolutions but can still consume significant data-rates. The following sections describe how the JPEG standard compresses digital images.

a. Transform RGB into Luminance and Chrominance

The CCD chips used in digital imagery collect a wide range of red, blue and green (RGB) lights, many of which are not discernable by the human eye. As a result, the unnecessary light values may be omitted without any perceptible decline in image quality. The RGB values are converted into a single luminance value and two chrominance values. The luminance value addresses the intensity of light while the chrominance value refers to the dominant hue and saturation. The YUV model is used to represent the RGB values. The Y value represents luminance, while the U and V values represent the chrominance values. The relationships between the values is shown in the following equations:

$$Y = 0.299R + 0.587G + 0.11B$$

$$U = 0.492\ (B - Y)$$

$$V = 0.877\ (R - Y).$$

b. Subsampling of Chrominance Values

The human eye is most sensitive to the intensity of light, or the "Y" value. As a result, the JPEG standard leaves the "Y" value unchanged. The chrominance value, on the other hand, is of lesser importance and can be discarded or changed with little effect on image quality. The JPEG algorithm discards several values to reduce the psychovisual redundancy and to reduce image size before compression occurs. This process is known as subsampling. For example, the 4:1:1 subsampling pattern encodeds only one pair of chrominance value for every four luminance values, resulting in only half the original number of bits

c. Group, Apply Discrete Cosine Transform, Quantize

Next, the JPEG algorithm groups the pixels into eight by eight blocks. The blocks are then ordered into a "raster-like" left-to-right, top-to-bottom scan pattern. The Discrete Cosine Transform (DCT) is then applied to each of the blocks and to each pixel. The result of the DCT is an average frequency value for each block of pixels and a frequency map of the block. The DCT for an M x N image is defined as:

$$F(u,v) = C(u)C(v)\sum_{m=0}^{m-1}\sum_{n=0}^{n-1} f(m,n)\cos(\frac{\pi(2m-1)u}{2M})\cos(\frac{\pi(2n-1)v}{2n}),_{0\le v\le N-1}^{0\le u\le M-1}$$

where C (U) is defined as

$$C(u) = \begin{cases} \frac{1}{\sqrt{M}}, \text{ if u = 0} \\ \frac{2}{\sqrt{M}}, \text{ if } 1 \le u \le M\text{-}1 \end{cases}.$$

and C (v) is defined as

$$C(v) = \begin{cases} \frac{1}{\sqrt{N}}, \text{ if v = 0} \\ \frac{2}{\sqrt{N}}, \text{ if } 1 \le v \le N\text{-}1 \end{cases}.$$

Next, the JPEG algorithm quantizes DCT values and rounds them to the nearest integer value using separate "quantization coefficients" described in the JPEG standard. After the values are quantized and rounded, they are ordered according to the zig-zag scan shown in Figure 18.

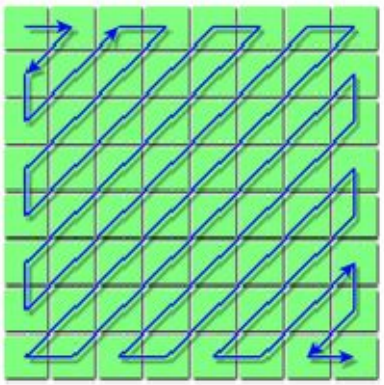


Figure 18. Zig-Zag Scan Method

d. Run-length Encoding and Secondary Coding

The zig-sag scan results in a bit-stream that is then converted into run-length pairs forming an intermediate symbol sequence. The "run" portion of the pair addresses the distance between non-zero coefficients in the block. The "length" value refers to the value of the non-zero coefficient immediately following a run. Finally, the JPEG algorithm uses either Huffman or arithmetic coding to compress the intermediate symbol sequence (Gibson et al., 1998). The arithmetic coding requires an expensive license and offers only minimal improvement over the Huffman Coding. Huffman coding is the default method used by the JPEG standard. After the intermediate bit-stream is coded, the image is fully compressed.

2. MPEG

The Moving Pictures Expert Group (MPEG) has released several digital multi-media compression standards that build upon one another. The most recently released MPEG standard is the MPEG-4 standard, which was released in 1999. As with JPEG, the MPEG-4 standard is considered lossy because RGB data are discarded. MPEG-4, however, further discards data through inter-frame predictive coding. As a result, MPEG-4 encoding significantly reduces throughput requirements. The MPEG-4 compression standards take advantage of spatial and psychovisual redundancies associated with displaying images and use advanced coding techniques to allow high quality video to be transmitted over limited bandwidth communication lines. The following sections briefly describe the MPEG-4 encoding process.

The first steps in the MPEG encoding process are similar to the JPEG encoding. The CCD chip captures light and turns the electrical signals into RGB values. Next the RGB values are converted into the YUV format and then are further sub-sampled to reduce the data requirements. Then the pixels are grouped into eight-by-eight blocks and a DCT is performed on each element. At this stage, MPEG differs significantly from JPEG.

Because MPEG-4 is a compression standard designed for all multimedia formats, the compressor and decompressor must be able to process multiple sources of data. The results of the DCT are organized into three different objects: video object, still texture object, and face object. The algorithm codes the objects into hierarchical layers, which build upon one another to enhance special and temporal resolution. This allows the compressor to distinguish between various objects within the video picture. As objects are distinguished, the compressor can allocate more data space for objects that require it, such as objects in motion. For example, if the objects in the background remain stationary, they might only be coded once and the foreground objects would be coded as needed. Since the foreground objects tend to be only a fraction of the total video, the allocation results significantly increase compression efficiency (Adam, 2002).

Furthermore, MPEG uses inter-frame predictive coding to reduce temporal redundancy. This is accomplished using the IPB frame model. The "I" frames are still frames of the scene. "P" frames are a statistical estimation of what the next frame will look like based on previous frames. "B" frames are coded based on comparing the eight-by-eight pixel blocks for the "I" and "P" frames. The MPEG video compression algorithm reduces the redundancies in digital video to compress video streams to a manageable size. Although the initial steps are similar to JPEG encoding, the use of inter-frame predictive coding allows MPEG standards to reduce the amount of data needed significantly to transmit and store digital imagery.

Understanding the processes that provide video from a remote sensor to the watch-stander is an important part of network design. This chapter introduced the basic concepts of digital video technology. The fundamentals of video capture were covered

followed by the bandwidth considerations associated with digital video data. Lastly, this chapter introduced and discussed the existing video compression techniques used to make digital video transmission and storage possible.

IV. DESCRIPTION OF PROTOTYPED NETWORK

The inherent flexibility and the unique requirements associated with wireless sensor networks allow the network to be customized to the user's needs. The area of operation and the intended purpose of the network greatly affect network architecture. For the purposes of this study, the prototyped network is designed to support the needs of the NPS Coalition Operating Area Surveillance and Targeting System (COASTS) program. However, the design parameters are intended to apply to possible deployment scenarios world-wide. This chapter describes the operational scenarios as a part of the COASTS exercise and further details the design of the integrated sensor-camera network prototype.

A. COASTS 2006

1. COASTS Overview

The emergence and relatively low cost of commercially available wireless networking technologies, which support traditional peacekeeping, law enforcement, and non-governmental organization applications, such as humanitarian assistance and disaster relief, create potentially important operational and resource considerations for decision-makers.

The COASTS research and development program demonstrates the capability to rapidly deploy and integrate low cost, state-of-the-art, unclassified networked air, ground, and maritime sensors providing real-time sensor-to-shooter information to tactical and remote decision-makers. As coalition operations continue to increase, the ability to manage and to disseminate the collected intelligence data effectively from deployed assets becomes ever more vital. The first iteration of the COASTS program began in 2005. In addition to the benefits resulting from cooperative research and development endeavors, the COASTS initiative helped demonstrate US Pacific Command's

commitment to foster stronger multi-lateral relations in the areas of science and wireless technology with key Pacific Theater allies (COASTS Marine Corps Systems Command Proposal, 2006).

COASTS 2006 will advance research relative to low-cost, commercially available solutions while integrating each technology into a larger system in support of tactical action scenarios. The demonstration planned for May 2006, in Chiang Mai, Thailand, will have a first-responder, law enforcement, and counter-terrorism and counter-drug focus. Furthermore, the tactical information being provided from the deployed sensors will be fused, displayed, and distributed in real-time, to local (Chiang Mai), theater (Bangkok), and global (Alameda, California) command and control centers. This fusion of information validates using wireless communication mediums to support redundant links of the National Information Infrastructure, as well as test the "last mile" solution for the disadvantaged user.

Continuing with the previous iteration's research theme, this effort will again examine the feasibility of rapidly-deploying networks (Fly-away Kit) and sustainment in a hostile climatic (temperature, humidity, wind, etc.) environment. Network improvements will include:

- incorporation and testing of new 802.11 mesh LAN equipment
- refinement of a jointly-developed 3-D topographic shared situational awareness application called C3Trak
- integration of "satellite in a suitcase"─portable satellite communication equipment
- enhanced unattended ground and water-based sensors
- new balloon and UAV designs
- portable biometric devices, portable explosive residue detecting devices
- revised operational procedures for deployment of the network.

COASTS 2006 field experiments will focus on several emerging sensor-to-shooter technologies and capabilities. The field experiments will be a part of the Lawrence Livermore National Laboratory (LLNL) Virtual Test Bed concept and are part

of an effort to link existing national and international Data Fusion Centers to promote and to enhance common information environments. COASTS 2006 experiments will occur in areas such as:

1) Maritime domain protection/awareness
2) Riverine and littoral warfare
3) Maritime Interdiction Operations (MIO)
4) Knowledge Database Design (KDD)
5) Wireless network technologies
6) Hastily formed networks
7) GPS tracking technologies
8) GPS Denied tracking technologies
9) Unattended, integrated sensor-camera networks
10) Wearable computing devices
11) Unmanned aerial vehicles (UAV)
12) Situational awareness applications
13) Persistent intelligence, surveillance, reconnaissance
14) Network security
15) Biometric collection devices
16) Modular network Fly-away Kits (FLAK).

2. COASTS 2006 Scenario

The COASTS 2006 network topology, illustrated in Figures 19 and 20, will be demonstrated in several operational contexts and field experiments. Two demonstrations will be conducted in the United States in conjunction with US Coast Guard and other Department of Defense organizations. Two additional demonstrations will occur in northern Thailand in partnership with the Royal Thai Armed Forces. The scenario will entail using deployed assets to support U.S. and Thai military and law enforcement forces in the detection, surveillance, interdiction/destruction, and post-hostility assessment of a maritime terrorist smuggling operation. This section provides an overview of the COASTS 2006 scenario based upon the COASTS 2006 Concept of Operations (CONOPS) and emphasizes the role of an integrated sensor-camera network to provide persistent intelligence, surveillance, and reconnaissance capabilities.

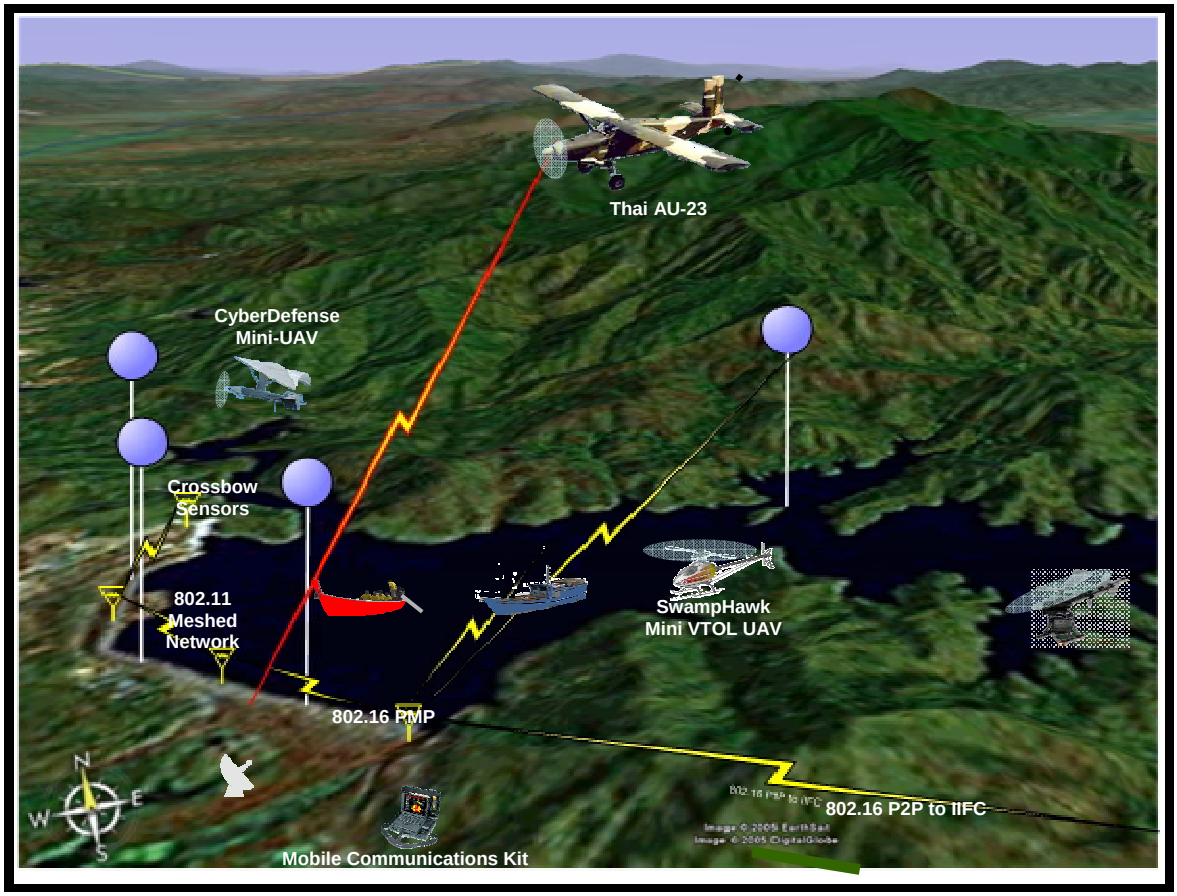


Figure 19. COASTS 2006 Topology at Mae Ngat Dam, Thailand

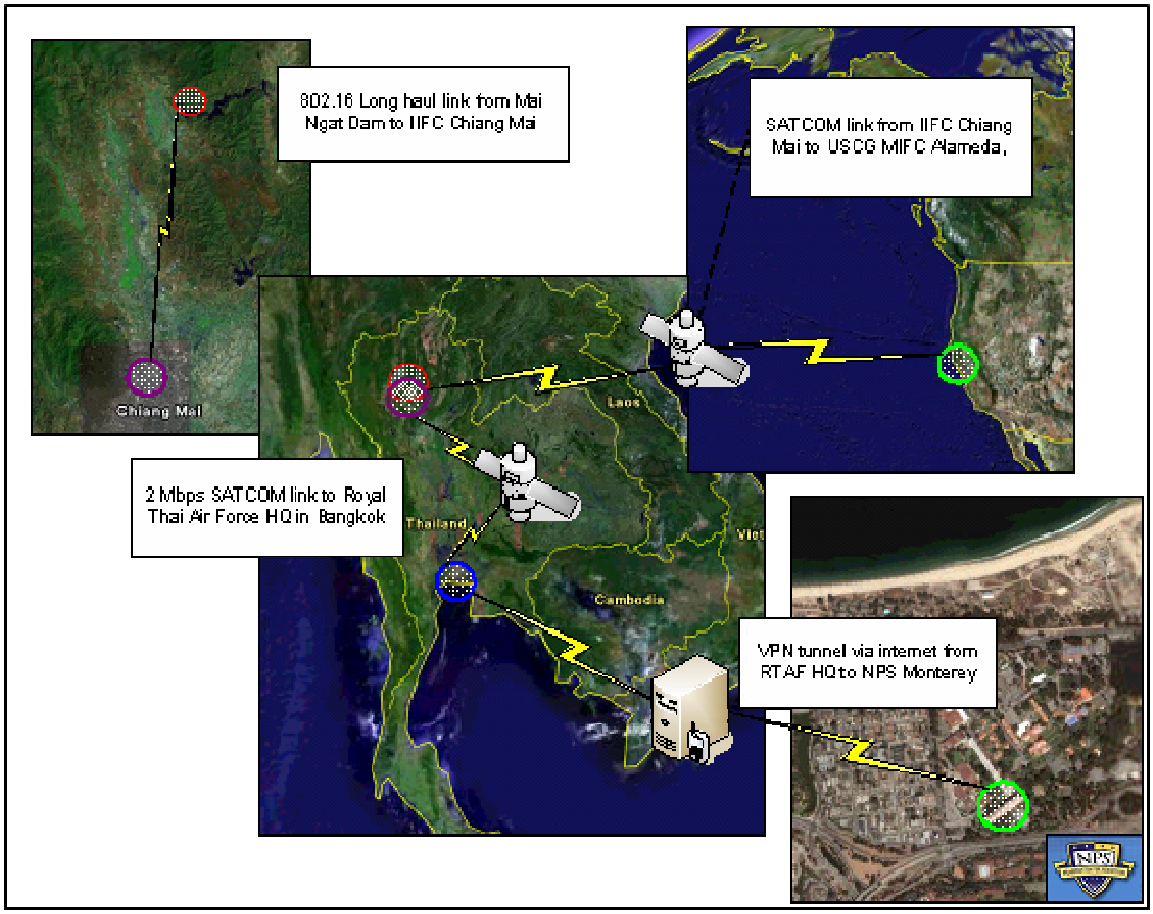


Figure 20. COASTS 2006 Global Network Topology

The scenario simulates a counter-drug and counter-terrorism operation. Intelligence indicates a suspected shipment of drugs and explosives will occur. The arrival of a longboat suspected of involvement in drug and arms smuggling operations will be detected by various unattended sensor suites deployed at a tactical waterborne choke-point. When triggered by the motion of the longboat, the sensors will send an automatic system alert through the C3Trak Shared Situational Awareness application. This system alert will be observed by all the tactical forces connected to the network, and by the various command and control (C2) centers.

When the longboat arrives at a "drop-point" the drug and explosive shipment will be transferred into the cargo bed of two awaiting trucks. An unidentified malefactor will be given a CD, which details the smuggling operation and financial ties with terrorist

organizations. This entire process will be remotely monitored through ground-based video cameras and aerial surveillance platforms. The surveillance video will be displayed at the local, regional, and strategic C2 centers.

After the transfer is complete, the scenario then splits into two parts. One part will entail the malefactor being tracked on foot by a Royal Thai Army and Police squad. The bad actor will cross land-based sensor-camera suites, again initiating a C3Trak system-wide alert. The IIFC will order the interdiction squad equipped with a wearable computing device, which can access all network data, and biometric and explosive residue collection capabilities to coordinate the apprehension of the suspected bad actor.

Simultaneously, the second part of the scenario will involve the convoy being tracked by the integrated sensor-camera networks. As the vehicle convoy exits the area, they will cross a sensor grid, deployed alongside the road, sending another C3Trak system-wide alert. At this point, orders will be passed from the strategic C2 center to capture all monitored units: longboat, trucks, and bad actor.

After the malefactor is apprehended, biometric data are gathered and passed to the MIFC for identity verification. Once positive confirmation is received that the captive is the high value target in question, the coalition ground forces holding the malefactor pass initial intelligence from the CD (captured with the malefactor's personal effects) and initial custody status via C3Trak to all network users. As the vehicle convoy crosses a final sensor-camera grid, a watch officer orders an air-to-surface strike. Concurrently, coalition maritime interdiction teams apprehend the long-boat. The scenario ends after all the malefactors have been captured or destroyed.

The COASTS 2006 scenario provides the foundations for designing an integrated sensor-camera network. The operational context of the COASTS 2006 represents common challenges and needs for deployment in any military or law enforcement application. The exact requirements for the COASTS program were determined, and then an extensive market survey was conducted to select the components needed for the network. More detailed information concerning the COASTS program can be found in

Appendix A, the COASTS Concept of Operations (CONOPS). The following sections introduce and describe the components selected to build the integrated sensor-camera network.

B. INTRODUCTION TO CROSSBOW

The sensor network components selected to build the sensor-camera network are produced by Crossbow Technologies. Crossbow is an established company focusing on sensing technologies. They are considered "a leading supplier of inertial sensor systems for aviation, land, and marine applications and other instrumentation sensors as well as the leading full-solutions supplier in the wireless sensor networking arena and the only manufacturer of smart dust wireless sensors (www.xbow.com)." Crossbow offers a variety of commercial sensor network hardware and software developed for security related applications.

C. SENSOR NETWORK COMPONENTS

The sensor components selected for use are the Crossbow MSP410CA Mote Security System. The MSP410 Mote Security System is a battery-powered, eight-node kit designed specifically for security applications and is shown in Figure 21. The solution is the wireless sensor network component of the integrated sensor-camera network. The robust mesh network and sensing capabilities provided by the MSP410 nodes provide the necessary ability to detect objects in an adverse environment. The following sections describe the intended deployments and components of the MSP410 Mote Security System

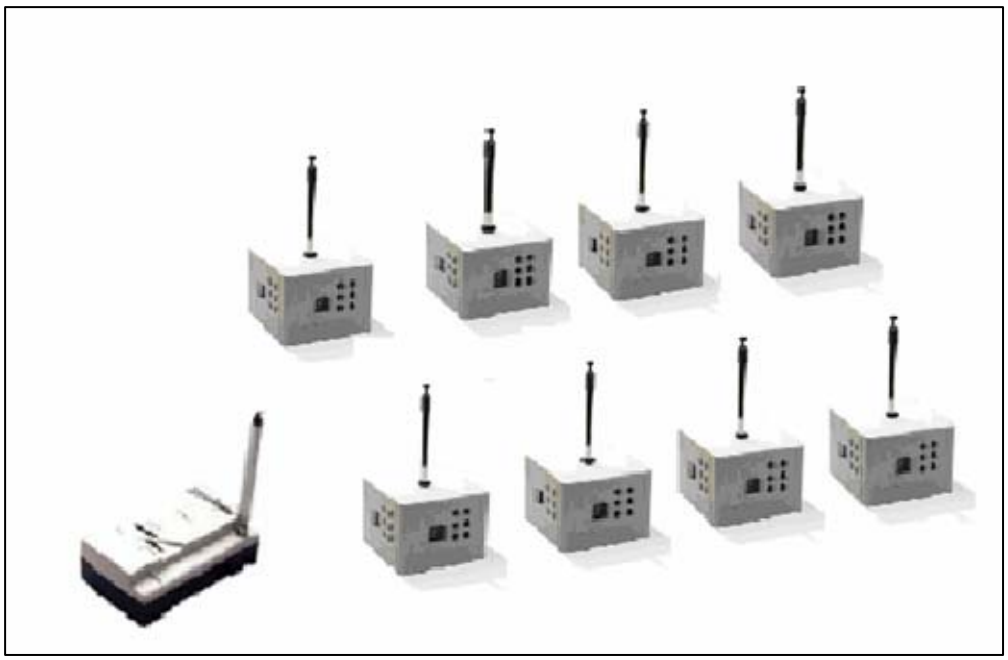


Figure 21. Crossbow MSP410CA Mote Security System

1. Proposed Deployments

The MSP410 Mote Security System is designed specifically for security related applications such as "remote border security, perimeter protection, intrusion detection and identification, and building occupancy monitoring (Crossbow, 2005)." Crossbow recommends two architectures. The first proposed deployment architecture is perimeter protection pattern. The company recommends the motes be deployed approximately 40 feet apart around the perimeter. They also recommend that the motes be oriented in the same direction. The perimeter protection design is illustrated in Figure 22.

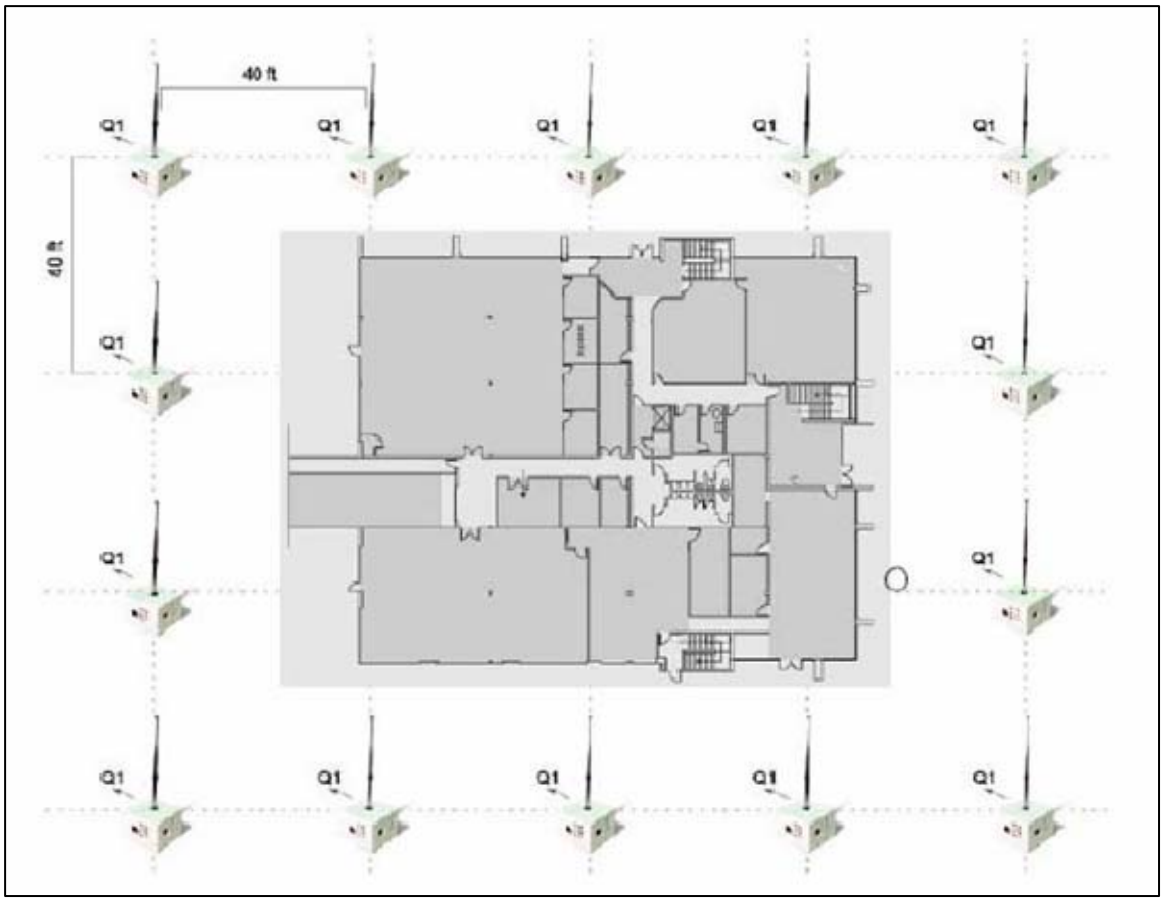


Figure 22. MSP410 Perimeter Deployment from MSP410 Series User's Manual (From: Crossbow, 2005)

The second deployment architecture suggested by Crossbow is the dense deployment grid. The dense deployment grid is designed to provide coverage in an area of interest such as an open field or anywhere that requires overlapping sensing areas. The distances recommended are based on the sensor coverage area and are not limited by communication distances. If overlapping coverage areas are not required, the distances can be increased to cover a greater area with the same number of nodes. The recommended dense deployment grid is shown in Figure 23.

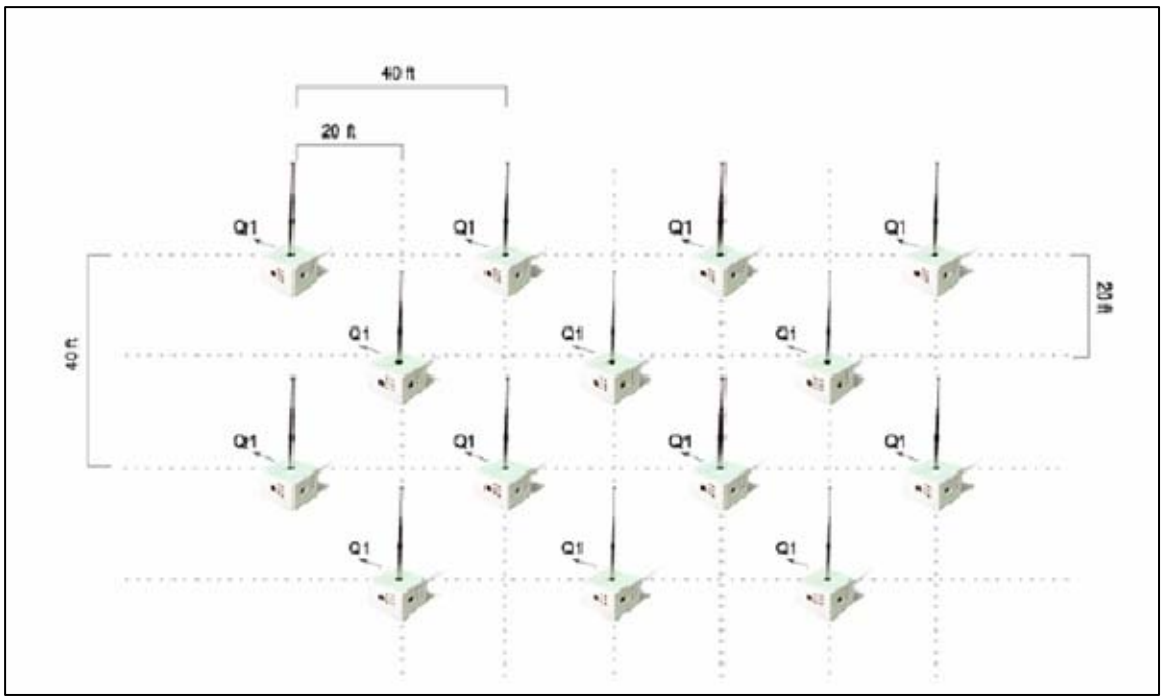


Figure 23. MSP410 Dense Deployment Grid from MSP410 Series User's Manual (From: Crossbow, 2005)

2. MSP410CA MICA2 Platform Core

The MICA2 processor and radio board is the heart of the MSP410 mote system. The MICA2 board is the core element of the nodes of the MSP410 WSN and is shown in Figure 24 as enclosed in the protective plastic case.

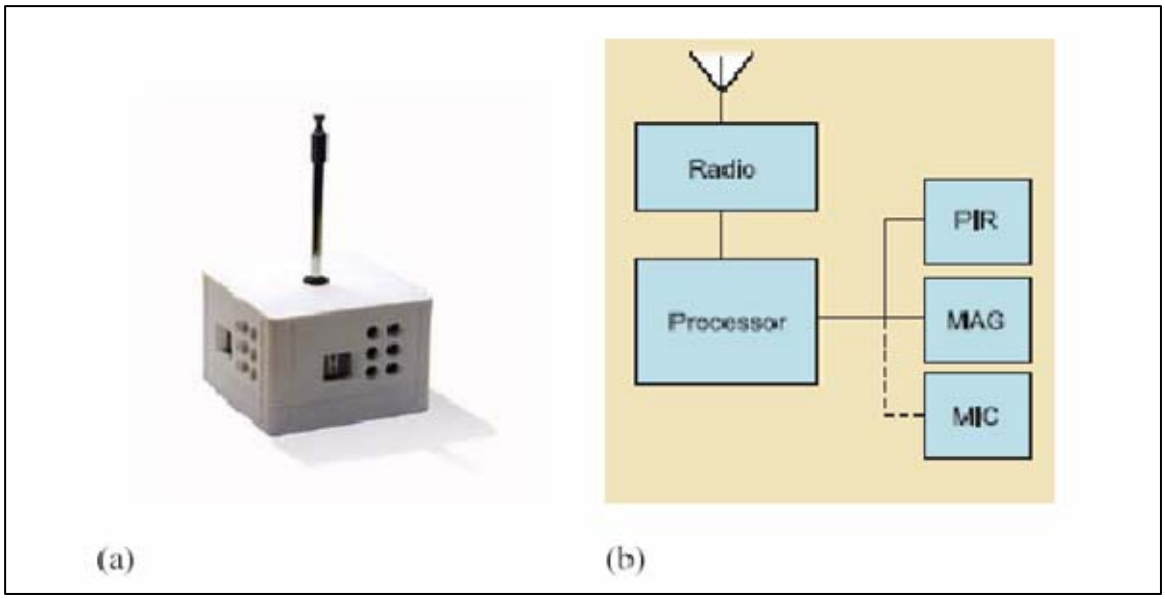


Figure 24. (a) High-level View of a Mote and (b) Block Diagram of Mote Components from MSP410 Datasheet (From: Crossbow, 2005)

The MICA2 processor and radio board controls the sensing and transmission capabilities of the mote. The processor is responsible for controlling the processing and logic tasks such as power management. Three variations of the MICA2 board exist based on the transmission frequency. The MPR400 is based in the 915 MHz range. The MPR410 operates in the 433 MHz range. The MPR420 operates in the 315 MHz range. The MSP410 Mote Security Systems sold in the United States uses the MPR410 MICA2 board and operates in the 433 MHz range. Figure 25 shows the circuit board and provides a block diagram for the MICA2 platform core.

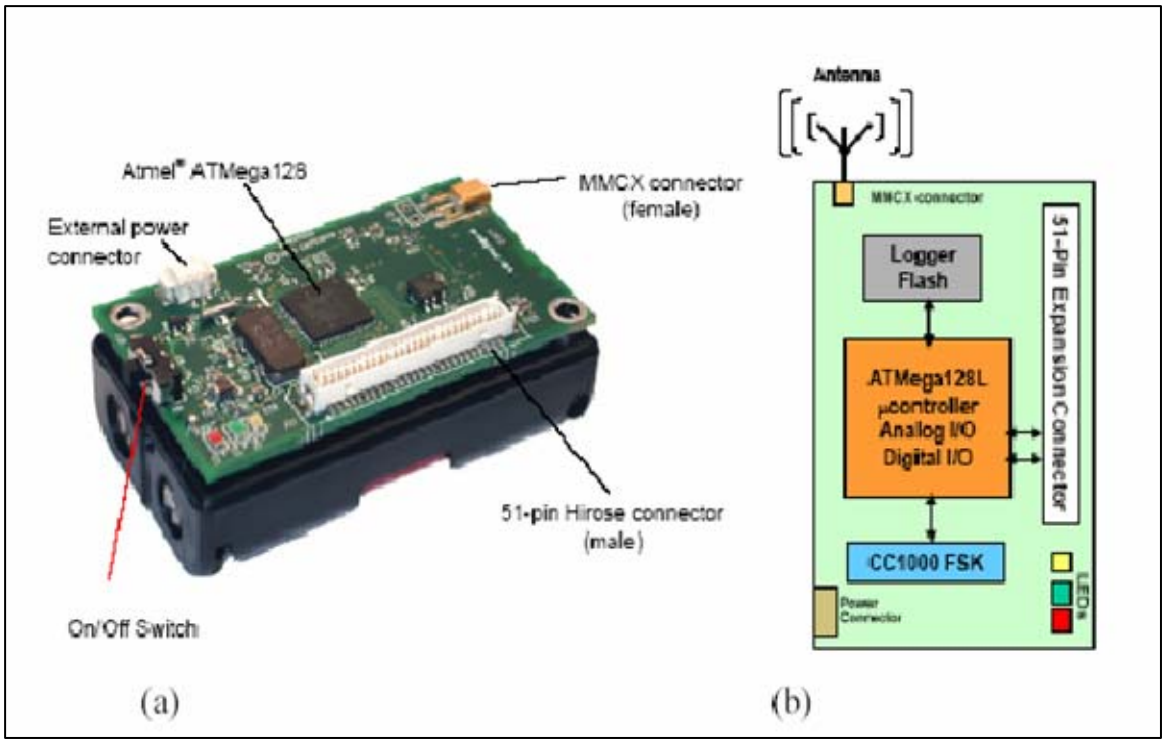


Figure 25. (a) MICA2 Platform Core without Antenna, (b) MICA2 Core Block Diagram from MPR/MIB User's Manual (From: Crossbow, 2005)

The Amtel Atmega 128 microcontroller is the processor chip and has total control over the function of the mote. Two peripherals are associated with the processor: a 64-bit Serial Identification Number and a 4-Megabit external flash. All sensor subsystems and any external devices are connected through external interfaces to the processor.

The MICA2 chip has green, yellow, and red Light Emitting Diodes (LEDs), which are used to provide visual status indications. The LEDs are controlled using general purpose input-output pins connected to the processor. However, when the processor board is inside the protective housing, viewing the LED indicators is difficult. Wired communication and mote reprogramming is accomplished using a 51-pin Hirose interface connector.

The MICA2 Platform Core also contains a Chipcon CC1000 radio. The Chipcon CC1000 radio uses two-tone FSK and Manchester encoding to operate at a baud rate of 19.2 kilobits per second (kbps). The standard radio configuration uses four channels with a recommended channel spacing of 500 kHz around the 433 MHz band. Although the

transmission power can be changed by reprogramming the chip, the default transmission power is set to the maximum level. According to the MSP410 User's Manual, the radio is capable of achieving radio ranges of "at least 250 feet on flat concrete ground and 150 feet when placed on grassy terrain with rolling hills."

3. MSP410CA Passive Infrared Sensor

In addition to the MICA2 core, the MSP410CA nodes contain several sensors, which serve to interface with the surrounding environment and gather data. The passive infrared (PIR) sensor is the most powerful sensing subsystem in the MSP410 package. The PIR subsystem provides 360º coverage using four sensing elements placed at the four corners of the MICA2 board. The PIR elements are designed to detect motion of objects that radiate thermal energy. Each element generates a ± 15º vertical viewing angle and a ± 45º horizontal viewing angle. The horizontal field of view is further subdivided into nine individual "beams." A "detection event" occurs when an object crosses one or more of the beams. This produces a shadow that crosses from one sensing element to the next. The sensor output is a signal proportional to the difference between the infrared energy striking the two sensing elements. Moreover, the PIR elements provide a "Quad Detect" capability. This allows the sensors to embed the quadrant that detected the object. From the quadrant information one can extract which direction the object is moving.

The MSP410 Series User's Manual states that the outputs of the PIR sensor are affected by the sensor's sensitivity, the sensor's position and elevation, the ambient thermal noise (temperature), and the objects characteristics. The sensors use filters to increase performance by reducing the effect of ambient thermal noise. Additionally, the sensors use "active filtering" to eliminate the monitoring bandwidth in the area where they have the greatest sensitivity from .01 Hz to 15 Hz. Table 3 summarizes the PIR subsystem specifications based on the MSP410 Series User Manual (Crossbow, 2005)

Specifications- Performance	Value	Comment
Optical Wavelength	5 μm to 4 μm	
Optical Bandwidth	.01 Hz to 15 Hz	
Vertical Field of View	± 15º	
Horizontal Field of View	± 45º	
Storage Temperature	-55º C to +125º C	
Human Detection Range	30 to 40 feet	Based on Sensor elevation of 3 feet above the ground and at 7º C (44. 7º F)
Vehicle Detection Range	50 to 60 feet	
Large Vehicle Detection Range	70 to 80 feet	

Table 3. Sensor Specifications Based on the MSP410 Series User's Manual (From: Crossbow, 2005)

4. MSP410CA Magnetic Sensor

The second sensing system in the MSP410CA nodes is the magnetic sensor. The magnetic detection subsystem consists of a two-axis magnetic field disorder detector. The magnetic sensor is activated when an object disturbs the local magnetic field. The magnetometer uses 100 Hz low-pass filters and two-stage amplification to minimize false detections while increasing the maximum detection range. Table 4 lists the magnetometers capabilities based on the MSP410CA User's Manual.

Parameter	Typical Value	
Bridge Resistance	1100 Ohms	
Field Range	± 6 gauss (Earth's Field = 0.5 gauss)	
Sensitivity	1 mV/Vgauss	
Linearity Error (Best fit straight Line)	± 1 gauss	0.05% FS
	± 3 gauss	0.4 FS
	± 6 gauss	1.6% FS
Bandwidth	DC to 5 MHz	
Noise Density	50 nVsqrt Hz at 1kHz	
Resolution	120 μgauss at 50 Hz Band Width	
Storage Temperature	-55º C to 175º C	

Table 4. Linear Magnetic Field Sensor Specifications (From: Crossbow, 2005)

5. Power Characteristics

As part of the MICA2 family, the motes in the MSP410CA are designed to be powered using two AA batteries. The MICA2 board requires a minimum of 2.7 Volts and a maximum of 3.6 Volts. Theoretically, the board can be powered using any source that provides direct current (DC) power within the defined range. Additionally, the board can be powered using the 51-pin Hirose connector and the two-pin Molex connectors. However, this is not a viable option due to the protective enclosure. The Crossbow supplied user's manual states that the motes will normally operate for ten hours on two AA batteries. Table 5 details the power consumption characteristics of the various aspects of the MSP410 motes.

Circuit	Mode	Current Required
PIR	Off	1 μA
PIR	On	300 μA
Magnetometer, per axis	Off	1 μA
Magnetometer, per axis	On	3 μA
Radio	Off	1 μA
Radio	Receive Mode	8 mA
Radio at 1 mW	Transmit Mode	16 mA
Processor	Sleep	15 to 20 μA
Processor	Active	8 mA
Serial Flash Memory	Write	15 mA
Serial Flash Memory	Read	4 mA
Serial Flash Memory	Off	2 μA

Table 5. Consumption Characteristics (From: Crossbow, 2005)

6. MBR410CA Mote Base Station

The base station that comes with the Mote Security System is the MBR410 serial base station. The MBR410 Base Station package, shown in Figure 26, consists of an MIP510 serial gateway connected to a MICA2 series MPR410 radio and processor board. The MICA2 processor board is programmed with a node identification of "0," forcing it to behave as a base station or network coordinator.

The MBR410 aggregates the networks data and forwards the data to a computer for storage or manipulation. Data transfer and mote programming is achieved through a standard RS-232 serial interface. The interface is a single channel, bid-directional interface with a DB9 connector. Power is supplied through an external power adapter, which plugs into a wall socket.

Figure 26. MBR410 Base Station for the MSP410CA Security System

D. CROSSBOW SOFTWARE

Crossbow Technologies has developed several software applications used extensively as a part of the MSP410 Mote Security System and during the testing and evaluation process. The important Crossbow-supplied software solutions are described in the following sections.

1. XMesh Network Stack

The XMesh Network Stack is the Crossbow developed sensor network protocol developed to support wireless sensor network. XMesh is an open-architecture, flexible and powerful, embedded wireless networking and control platform built on top of the TinyOS operating system. It uses proven mesh routing techniques and reduces the number of messages sent through the network. This reduces power consumption and significantly extends the battery life of the system. The XMesh protocol is designed to be completely compatible with the IEEE 802.15.4 and ZigBee standards.

2. XServe

XServe is a powerful command-line software component that provides remote data logging capabilities. WSNs use streamlined message formats and network protocols to reduce the amount of power and memory needed for communications. Traditional

internet protocol (IP)- based networks do not use the same formats or protocols. XServe acts as a translator between the two networks and allows sensor network data to be passed over traditional IP networks (MOTE-View Users Manual, 2005).

3. MOTE-View

MOTE-View is Crossbow's primary user interface for wireless sensor networks. It is designed to provide an intuitive graphical user interface (GUI) to control the motes and to view and log the sensor data. The MOTE-View software is extensively used in the testing procedures and operational scenarios conducted as part of this thesis. Mote-View is part of a three-layer network architecture developed by Crossbow. It serves as the client layer, where network data can be monitored, interpreted, and analyzed. The second layer is the server layer that logs data and makes them available locally or remotely. The third layer is the mote layer, which consists of the onboard sensors and the TinyOS operating system. The three-layer implementation is shown in Figure 27.

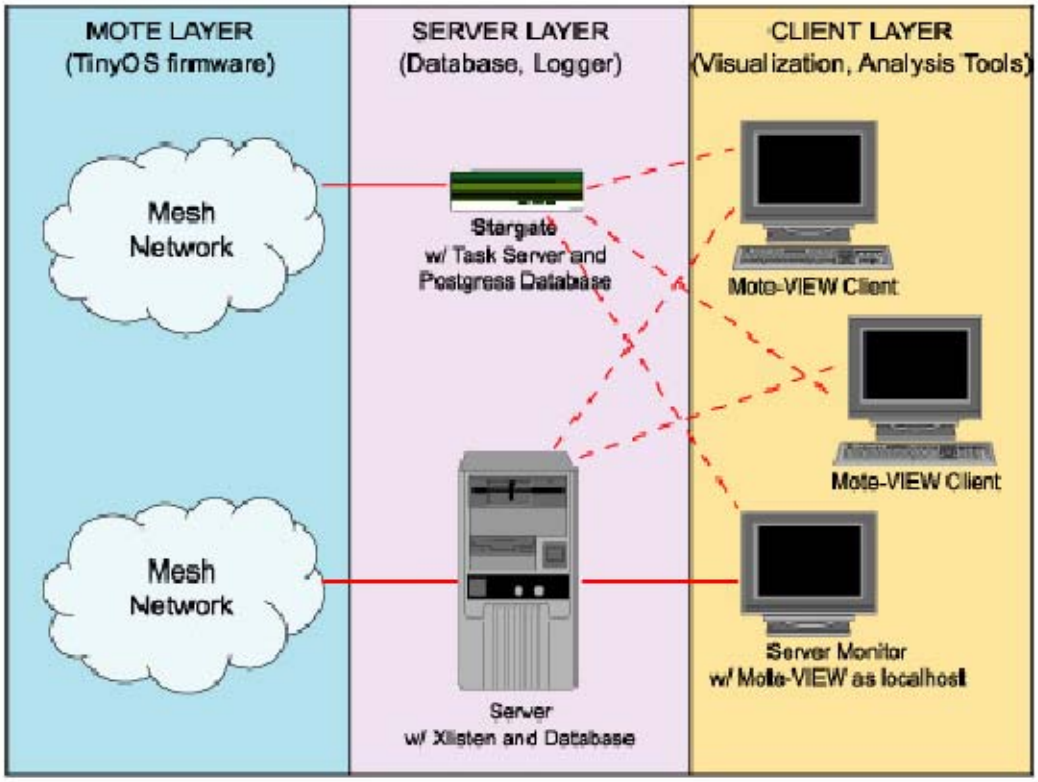


Figure 27. Layer Sensor Network Implementation from MOTE-View User's Manual (From: Crossbow, 2005)

MOTE-View provides several valuable ways to visualize the data received by the wireless sensor network. One method that is used is the "data log" view, which allows the data to be saved in a database. The most recent sensor data, node status, and any error messages are constantly updated. The software also has the ability to query the database to retrieve specific data sets. Figure 28 is a screenshot of the "data view" tab found in the MOTE-View software.

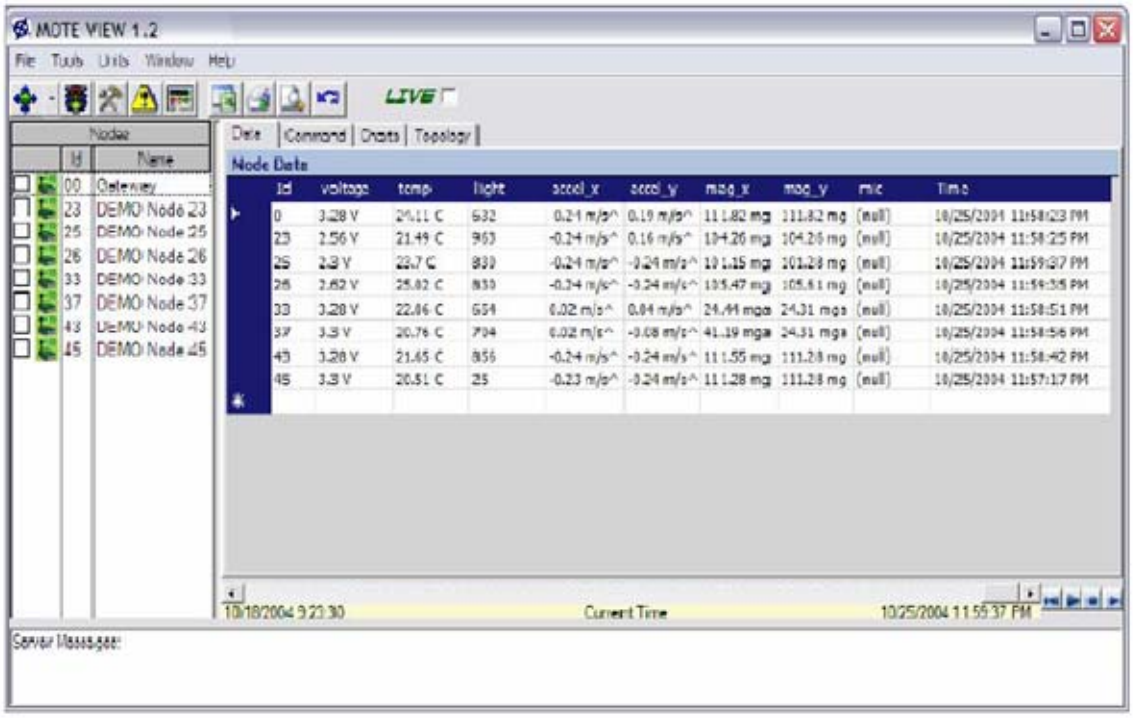


Figure 28. Screenshot of the Data View in MOTE-View

MOTE-View also provides the capability to view historical graphs of the data logged by the sensors by using the "Chart" view. The "Chart" view displays up to three graphs produced from a maximum of twenty-four nodes. Figure 29 is a screenshot of the "Chart" view in MOTE-View.

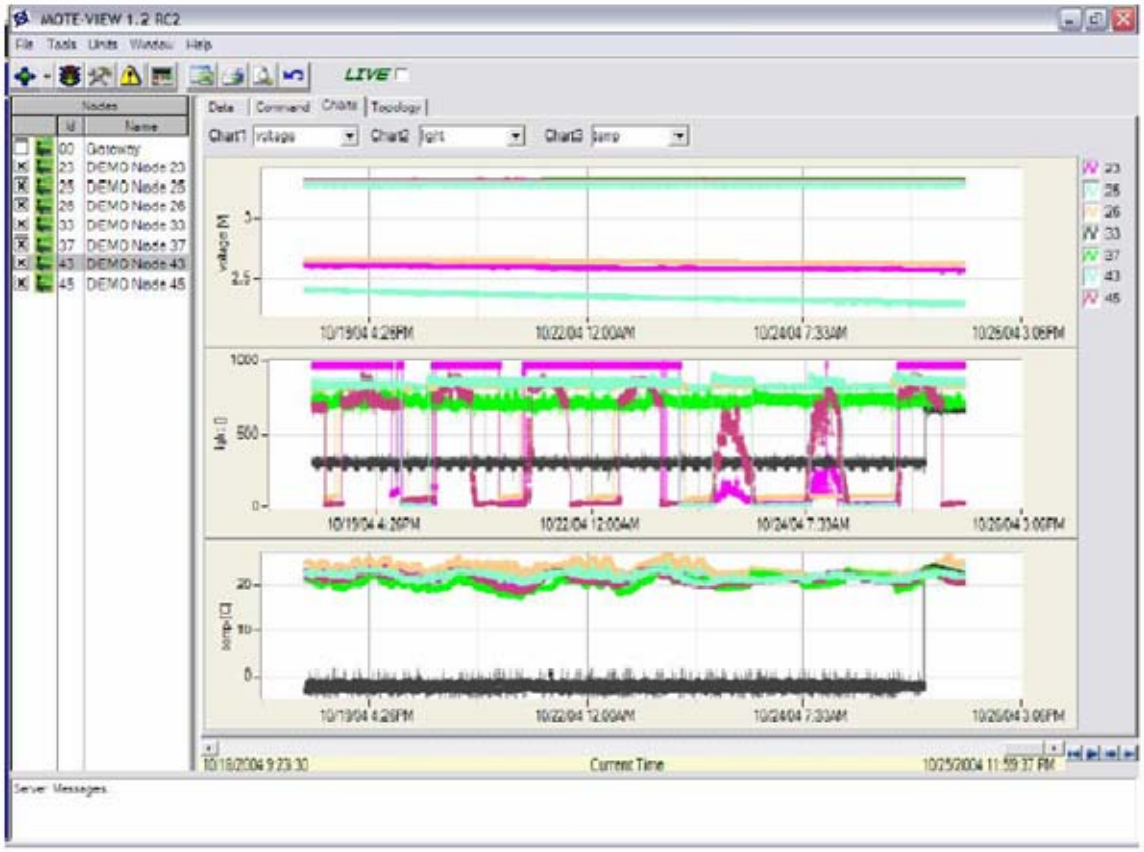


Figure 29. Screenshot of the Chart View in MOTE-View

The final graphical representation of the sensor network found in MOTE-View is the "Topology" view. The "Topology" view is a drag-and-drop view that allows the user to view the physical layout of the sensor network. The nodes can be placed in the same relative position as they are deployed. It displays all the network data including sensor values and parenting information. The "Topology" view also allows the user to import background images such as photographs or blueprints of buildings. Figure 30 is a screenshot of the "Topology" view.

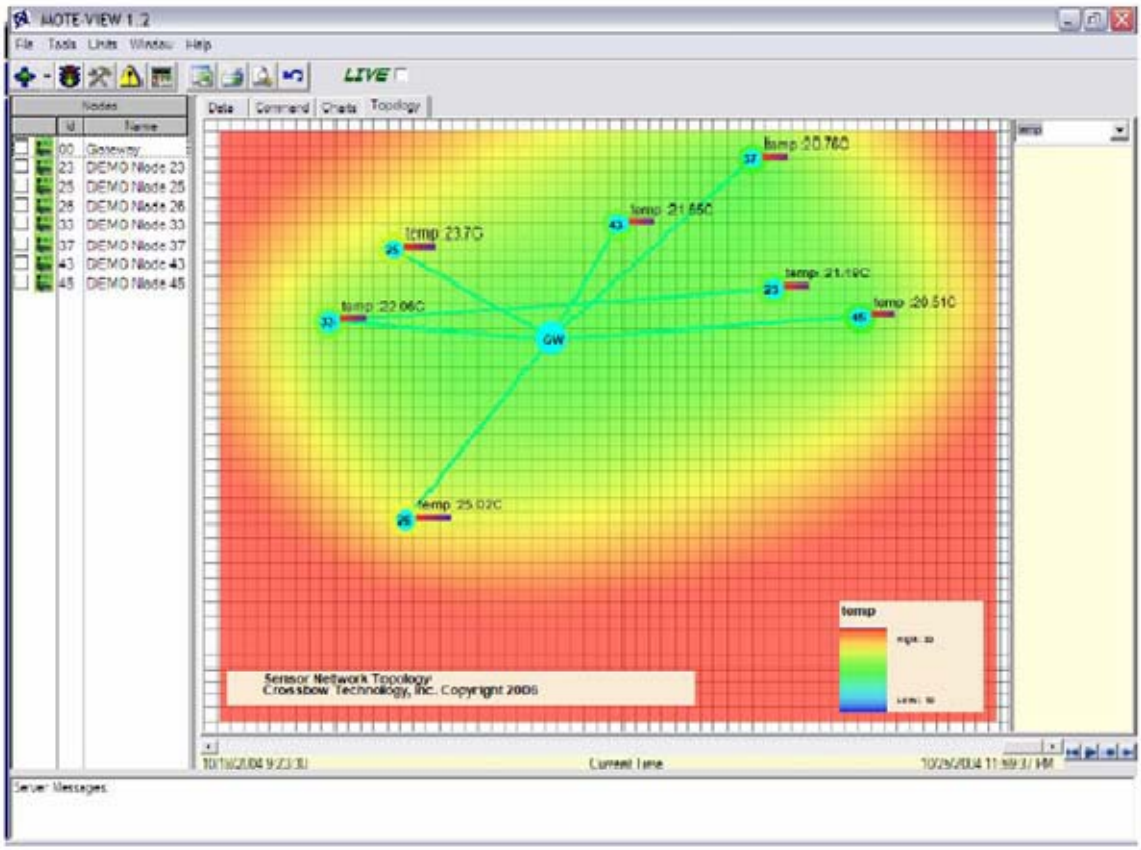


Figure 30. Screenshot of Topology View in MOTE-View

4. Surge View

Surge-View is another software solution provided by Crossbow Technologies. Although sensor data can be viewed using the program, Surge-View is primarily a GUI application designed to provide the user with networking information. The Sure-View software contains the Surge GUI, Stats, and HistoryViewer programs. The Surge GUI program, shown in Figure 31, allows the user to view connectivity and routing statistics. It also allows the network data to be saved to a local computer. The Stats program, shown in Figure 32, provides network health statistics. Finally, the HistoryViewer program (Figure 33) allows the user to replay graphical representations of the network's topology and statistics (Getting Started Guide, Crossbow, 2005).

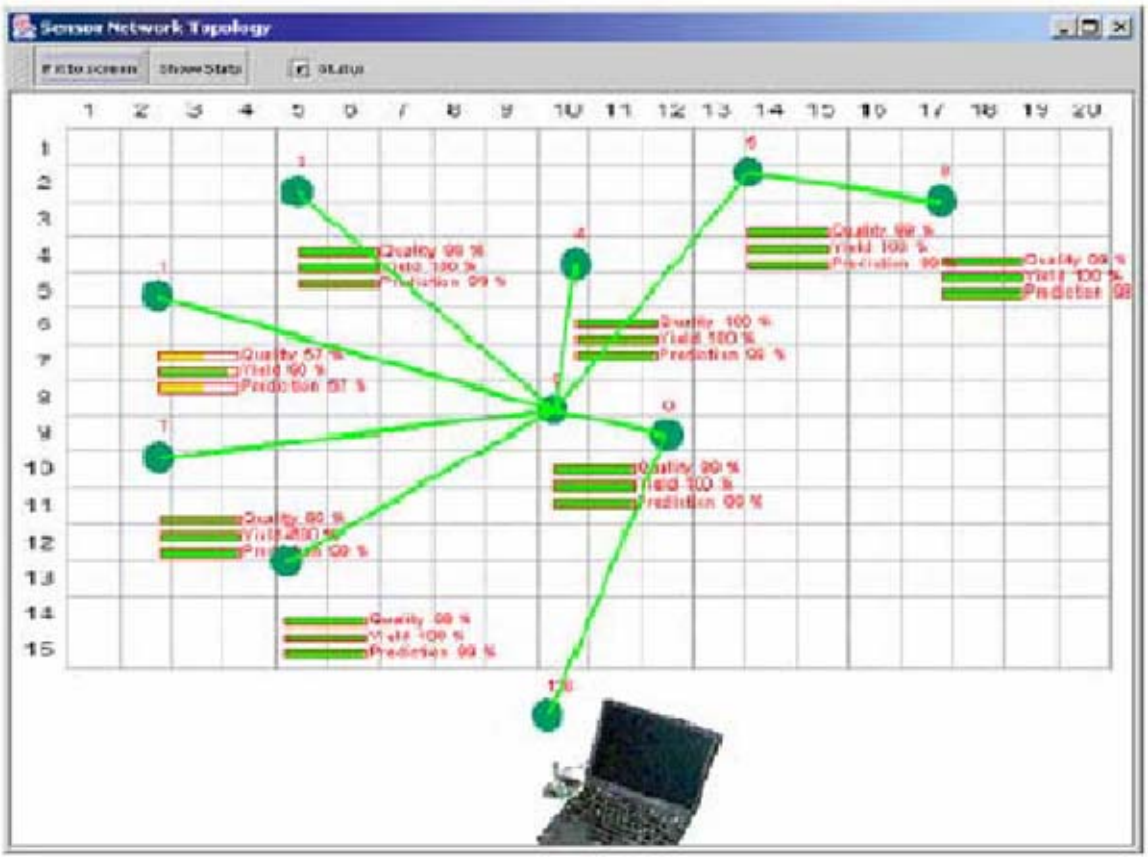
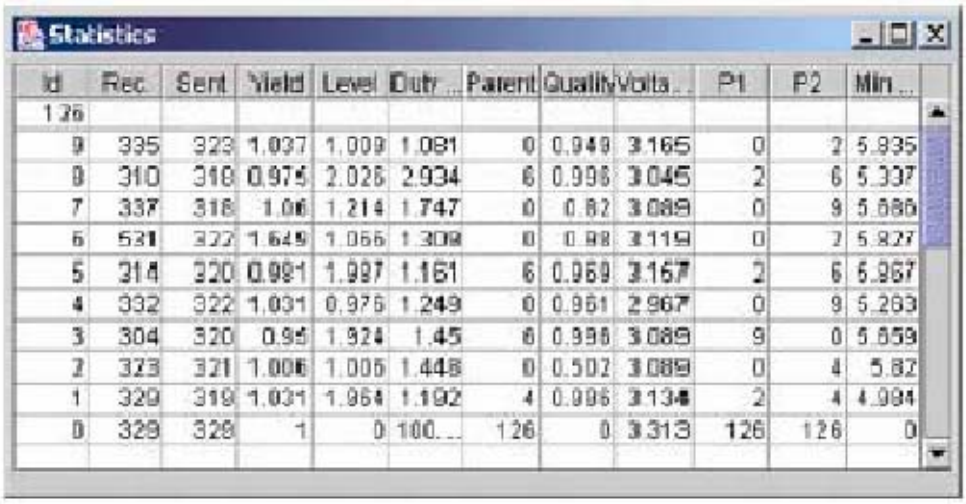


Figure 31. Screenshot of Surge GUI (From: Getting Started Guide, Crossbow, 2005)



Id	Rec	Sent	Yield	Level	Distr ...	Parent	Quality	Volta...	P1	P2	Min ...
126											
9	335	323	1.037	1.009	1.081	0	0.949	3.165	0	2	5.935
8	310	318	0.975	2.025	2.934	6	0.996	3.045	2	6	5.337
7	337	316	1.06	1.214	1.747	0	0.82	3.089	0	9	5.686
6	531	322	1.649	1.066	1.308	0	0.98	3.119	0	2	5.827
5	314	320	0.981	1.997	1.161	6	0.969	3.167	2	6	5.967
4	332	322	1.031	0.976	1.249	0	0.961	2.967	0	9	5.283
3	304	320	0.95	1.924	1.45	6	0.996	3.089	9	0	5.659
2	323	321	1.006	1.005	1.448	0	0.502	3.089	0	4	5.82
1	329	319	1.031	1.964	1.192	4	0.996	3.134	2	4	4.994
0	329	329	1	0	100....	126	0	3.313	126	126	0

Figure 32. Screenshot of Stat (From: Getting Started Guide, Crossbow, 2005)

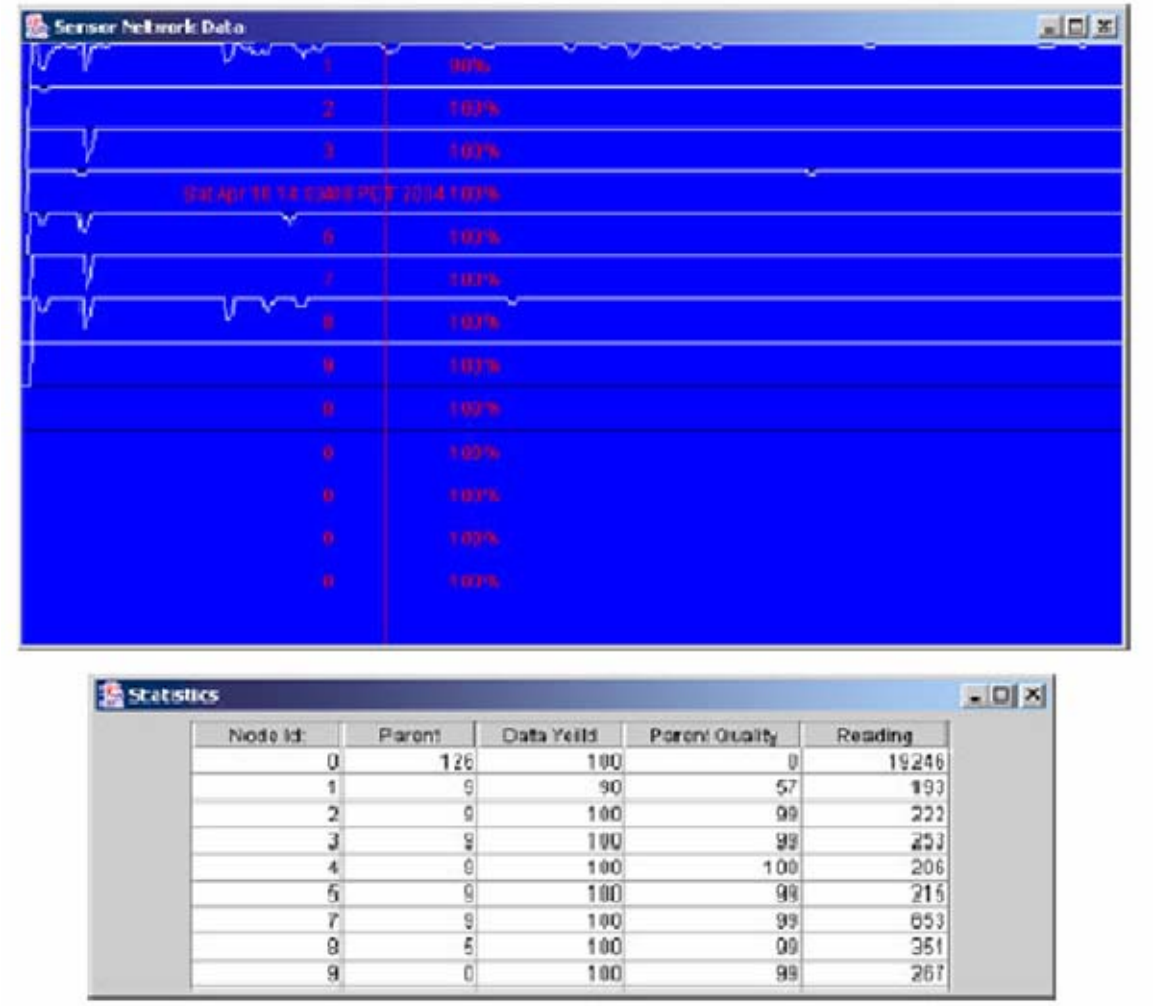


Figure 33. Screenshot (From: Getting Started Guide, Crossbow, 2005)

E. VIDEO NETWORK COMPONENT

The role of the cameras in the integrated network is to provide remote, real-time visual information to a watch-stander. This offers several key benefits, including visual verification of sensor activity, remote monitoring, and persistent surveillance. Providing real-time visual information assists decision makers in making accurate and timely decisions.

Numerous law enforcement and military organizations currently use video surveillance technologies on a daily basis. As a result, numerous commercial companies have begun developing video products designed for remote monitoring and security applications. Among the most prolific of such companies is Axis Communications,

which is a global market leader in network video products and specializes in "professional network video solutions for remote monitoring, security surveillance and broadcasting (www.axis.com/corporate/index.htm)."

The Axis 213 PTZ Network Camera, shown in Figure 34, is the video component selected for the integrated sensor-camera network. The camera was selected for several important reasons. Firstly, the Axis 213 camera is currently in use by several military and law enforcement organizations worldwide. It is currently in use by several United States military organizations such as the U.S. Air Force Force Protection Battle Lab. Additionally, the Axis 213 is currently used by the Royal Thai Armed Forces operations in support of the Global War on Terror. Secondly, the size and shape of the Axis 213 is conducive for covert operations and concealment. Thirdly, the camera does not consume significant amounts of power and can easily be powered for extended time periods on a common car battery. Finally, the Axis 213 provides significant performance capabilities in a single, cost-efficient package. The camera offers impressive pan, tilt, and zoom functions combined with built-in infrared capabilities, adjustable frame rates, multiple video stream formats, and preset viewing positions. Table 6 provides details of the important performance capabilities of the Axis 213 PTZ Network Camera.

Figure 34. Axis 213 PTZ Network Camera

Capability	Specification
Lens	1.5 – 91mm F1.6 –F4.0, motorized zoom lens Horizontal viewing angle: 42 – 1.7º Auto focus, 26x optical and 12x digital zoom
Minimum Illumination	Color mode: 1 lux, F1.6 IR mode: 0.1 lux, F1.6* *Using built in IR light in complete darkness up to 3 meters
Video Compression	Motion JPEG MPEG-4
Resolutions	704x480, 768x576, 160x120, 176x144
Frame Rates	Motion JPEG: Up to 30/25 frames per second MPEG-4: 30/25 or 21/17 frames per second
Video Streaming	Simultaneous Motion JPEG and MPEG-4 Controllable frame rate and bandwidth Constant and variable bit rate
Pan Angle Range	340º
Tilt Angle Range	100º
Zoom	26x optical, 12x digital
Preset Positions	20 operator definable preset positions and configurable monitoring sequence
Video Access	Up to 20 simultaneous clients
Supported Protocols	IP, HTTP, TCP, ICMP, RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, UpnP, ARP, DNS, DynDNS, SOCKS
Connectors	RJ-45 26-pin multi-connector
Power	13 V DC, max 24 W external power supply
Operating Conditions	5 – 40 ºC (41 – 104 ºF) 20 – 80 % non-condensing relative humidity
Dimensions (HxWxD) and Weight	130 x 104 x 130 mm (5.12 x 4.09 x 5.12 in) 700 grams (1.55 pounds)

Table 6. Axis 213 Capabilities from Axis User's Manual (From: Axis, 2005)

F. ADDITIONAL EQUIPMENT

The integrated sensor-camera network is intended to operate with both wired and wireless networks. However, finding the components with built-in wireless networking capabilities was impossible. As a result, two additional network components serve to integrate the sensor-camera network with a wireless network. The additional components are described in the following sections.

1. Vlinx Wireless Serial Server

The standard base station for the Crossbow MSP410CA system does not interface with an external wireless network. The only external interface is the standard serial connection. To interface with the existing COASTS wireless network correctly, a device is needed to convert the serial data from the base station to the standard 802.11 wireless data format. The Vlinx Wireless Serial Server is a product built by B&B Electronics to connect serial devices to existing 802.11 b/g wireless networks. The wireless serial server is designed for use in industrial environments and can be powered by AC or DC power supplies. Device configuration is achieved through a standard RJ-45 connection. The Vlinx server is capable of operating in "Direct IP" mode, "Virtual COM Port" mode, and "Serial Tunneling" mode. Direct IP mode allows the device to broadcast the serial data to a specified IP address using the TCP or UDP protocols. Virtual COM Port mode allows programs to extend their COM ports across a network effectively. The serial device will appear to be connected directly to the computer and programs will be able to access data as if the device was physically connected to the computer. Serial Tunneling mode allows two serial devices to communicate wirelessly with each other. During proof-of-concept demonstrations, the Vlinx serial server was used in Virtual COM mode, which allows the MOTE-View program to access the sensor data through a wireless network. During integration with the COASTS network, the Vlinx server is used in Direct IP mode and sends the sensor data to the situational awareness programming using the UDP data format. Figure 35 depicts the Vlinx ESR901W232 Wireless Serial Server.

Figure 35. Vlinx ESR901W232 Wireless Serial Server

2. Mesh Dynamics 802.11 Wireless Access Point

Like the sensors, the Axis 213 camera does not have wireless networking capabilities built-in. The Axis camera is designed to communicate with networks using an RJ-45 connection. As a result, a wireless access point is needed to connect the Axis 213 with a wireless network. The backbone of the COASTS network is an 802.11 mesh network. The Mesh Dynamics multi-radio backhaul access points are used to build a robust, high-speed wireless mesh network. Additionally, the Mesh Dynamics access points, shown in Figure 36, are used to connect the Axis 213 cameras using a standard Ethernet connection. The access points allow the seamless connection of video data to the wireless network. The Mesh Dynamics access points are well-suited for military applications because they are in weather resistant protective housings designed to operate in a wide range of temperatures. Additionally, the access points provide the flexibility to add multiple radios to provide efficient coverage of the operating area.

Figure 36. Dynamics Mesh Network Access Point

The addition of the Vlinx Wireless Serial Server and the Mesh Dynamics Access Point, allow the individual components of the integrated sensor-camera to operate wirelessly and to form the complete system. The entire system is composed of easily available COTS technology. The prototyped network can be quickly deployed and has a minimal logistics footprint. Figure 37 shows the network as deployed in the COASTS May 2006 demonstrations while Figure 38 shows the logistics footprint associated with the network.

Figure 37. Deployed Integrated Sensor-Camera Network

Figure 38. Logistics Footprint

This chapter introduced the COASTS 2006 Program. Furthermore, the COASTS operational scenario was discussed in depth. The COASTS scenario drove many of the requirements and design specifications of the integrated sensor-camera network. Finally, this chapter provided a detailed discussion of the individual components of the prototyped network.

THIS PAGE INTENTIONALLY LEFT BLANK

V. SELECTION OF METRICS AND EXPERIMENT DESIGN

The thorough testing and evaluation of systems is a critical component during the system's lifecycle. The selection of metrics and the effective design of testing procedures aid the decision makers during the system's lifecycle. Metrics must be consistent, quantitative, and measurable. Testing procedures must be scientifically designed to test the intended parameters in a meaningful manner. This chapter introduces the qualities of an effective metric. It also describes the metrics used to evaluate the prototyped sensor-camera network. Finally, this chapter describes the testing processes used in the evaluation process.

A. ATTRIBUTES OF AN EFFECTIVE METRIC

An effective metric is a "meaningful measure of the extent or degree to which an entity possesses or exhibits a particular characteristic (DACS, 2005)." Metrics are designed to measure the behavior of a system objectively and quantifiably. Although there are many attributes to a good metric, useful metrics have several key characteristics in common.

The first characteristic of a useful metric is that it can be observed and monitored over time. This characteristic requires that the metric be quantifiable. By observing and meaningfully quantifying a metric, one can analyze and compare network performance. Metrics should be interval data to allow for calculations, graphical representations, and comparisons. Nominal and ordinal values do not allow calculations and only allow for counting frequency of occurrences and ranking options. Nominal- and ordinal- based metrics essentially provide a "snapshot" of the system at a specific time. Although snapshots provide historical performance information, metrics that allow users to predict and to adjust performance in real-time are much more useful for networks. Interval-based metrics can be tracked and graphed, allowing one to characterize network performance visually. Network administrators can use the easily understandable metrics to adjust network parameters, such as sensor location or transmission power, and to optimize performance.

The second quality of an effective metric is that it consistently measures the same item. Consistently measuring the same item allows the data to be analyzed. Changing what is included in the metric invalidates the entire measurement and data collection processes. For example, throughput tests must use the same packet size to analyze bandwidth performance properly. Using different packet sizes will result in different bandwidth behavior and, therefore, provide inaccurate results.

Thirdly, taking actions to change the indicated performance must be possible. Metrics are often used to ensure that performance is within acceptable values. If a metric exceeds the acceptable value range, there must be actions to adjust the value. For example, if latency is too high, a network administrator must have actions to reduce the latency. Another example might be communication range. If the communication range between sensors is unacceptable, the administrator might take several actions to improve the range. For instance, the administrator might increase sensor elevation or adjust the transmission power until the desired ranges are met.

The final characteristic of an effective metric is that it must be able to be benchmarked against similar systems. Benchmark comparisons allow trade-off analysis between systems. For example, benchmark tests can compare a wireless sensor network to a traditional wired sensor network. This allows administrators to determine the effect of making changes to a system.

B. SELECTED METRICS

The successful evaluation of the performance of the integrated sensor-camera network was achieved through intensive data collection and analysis. The metric selection processes consisted of extensive market research and interviews with potential operational end-users. The metrics selected were chosen to offer the most beneficial performance indications. Additionally, metrics were selected to provide administrators with a tool to assist in designing the networks.

The first metric used throughout the operational experiments was the detection range of the sensors. Detection range is, perhaps, one of the most important sensor performance parameters. The detection range directly affects the usefulness of a sensor

network, the deployment architecture, the deployment density, and the deployment purposes. For example, imagine a sensor network is designed to detect vehicles at 100 feet. If, for some reason, the accurate detection range of the sensors falls to 80 feet, the network fails to meet its design objectives. Lapses in sensor coverage in a perimeter defense network pose a significant security risk to the organization. For the purposes of this experiment, detection ranges are measured in feet from the sensor. Several controllable factors are expected to impact the detection range. These factors include, but are not limited to sensor sensitivity, sensor elevation, object type, object speed, and environmental conditions.

The second metric used during the operational experiments is the RF communications break range. The break range is the distance at which radio communications between two sensors is lost. Break range impacts the deployment density and design objectives. Vehicle tracking is one potential military and law enforcement application of sensor networks. In a perfect world, operators would have enough sensor resources to track a vehicle through the entire area of interest. However, military and law enforcement agencies operate with a limited budget and often operate in extremely large operating areas. Sensor networks with higher break ranges allow operators to spread a limited number of sensors over a larger operating area for broad detection and monitoring capabilities. More accurate detection and monitoring can be achieved in specific areas by increasing the senor density in that area. The inherent flexibility of WSNs provides the ability to tailor sensor networks to unique applications easily. The controllable factors expected to impact break range are transmission power, receiver sensitivity, sensor elevation, terrain, and environmental conditions.

The third metric used is RF reassociation range and is similar to break range. The reassociation range is the distant at which two sensor nodes can locate each other and begin communicating. This metric is an important indicator of the survivability of mesh networks. WSNs are self-healing networks that often operate in adverse conditions. It is critical that the failure of a single node does not have a substantially negative impact on performance. Sensor network designers must ensure that a node is within the reassociation range of several other nodes. Take the example of a network in which only one node is communicating directly to the base station. That node is a single-point-of-

failure. If other nodes cannot reassociate with the base station, the entire network has the potential of being disconnected. The operator will be unable to access the sensor information. The controllable factors expected to impact reassociation range are identical to the break-range factors.

The probability of detection is the fourth metric used. Although probability of detection is difficult to measure instantaneously, it is extremely valuable when comparing the effectiveness of two systems and especially during network design. As a design tool, the probability of detection information allows network administrators to design sensor network architecture quickly to meet specific needs. As a comparison and analysis tool, the information allows decision makers to measure actual performance versus predicted performance and to choose the system that meets their needs. With respect to detection probability, two levels exist. The first level is the individual sensor-level. This refers to the probability that a single sensor can detect an object. At this level, the probability of detection depends largely on sensor sensitivity, object cross-section, object speed, sensor elevation, and the distance of the object from the sensor. The second level is the network-level. This refers to the probability that an object will be detected if it traverses the network as a whole. The network-level depends on the sensor-level probability of detection and the node density. This thesis focuses entirely on the sensor-level probability of detection.

The fifth metric used in analyzing the integrated sensor-camera network is link quality. Link quality is the ratio of the number of packets received to the number of packets sent between two nodes. Link quality is an indicator of the efficiency of a communications connection. Poor link quality is typically caused by network traffic congestion. Congestion, in turn, causes packet loss and often lowers the throughput. Packet loss can also result from bit errors caused by various link imperfections and improperly functioning equipment (Cottrel, et al.).

The final metric considered is the video frame rate. Frame rate can affect the timeliness and usefulness of the video being provided. In a persistent surveillance environment, bit rates that qualify as streaming-video are desirable. Low frame rates provide the possibility that an object might pass through the camera's field of view but no

image of the object will be captured. For example, if a camera is operating at one frame every five seconds, an object has four seconds to pass the camera without being captured on video. If the camera is operating at 30 frames per second, the object has one-thirtieth of a second to bypass the camera.

C. MEASURES OF EFFECTIVENESS AND PERFORMANCE

The selection of metrics allows the system to be benchmarked, tracked, and monitored. However, this only provides a quantitative comparison of the system's performance. Measuring the relative importance of aspects and to compare the over-all quality of a system is often necessary. Measures of Effectiveness (MoE) and Measures of Performance (MoP) are qualitative and quantitative values that allow for the impartial trade-off analysis.

When evaluating a system, it is important to break down the customers' requirements systematically to their most basic components and to ensure that those requirements are addressed in engineering specifications. This process requires both qualitative and quantitative measurements. MoE values represent the customers' requirements. They are typically qualitative in nature. Measures of Effectiveness use weighted values to represent the relative importance of the customers' requirements and expectations. Additionally, MoE values are often constructed in a hierarchical manner. For example, there might be three broad categories that are important to the user. Weighted values are assigned to these broad categories. The broad categories are then further decomposed into smaller units. This process repeats until the most basic components are reached. Figure 39 depicts a sample Measure of Effectiveness.

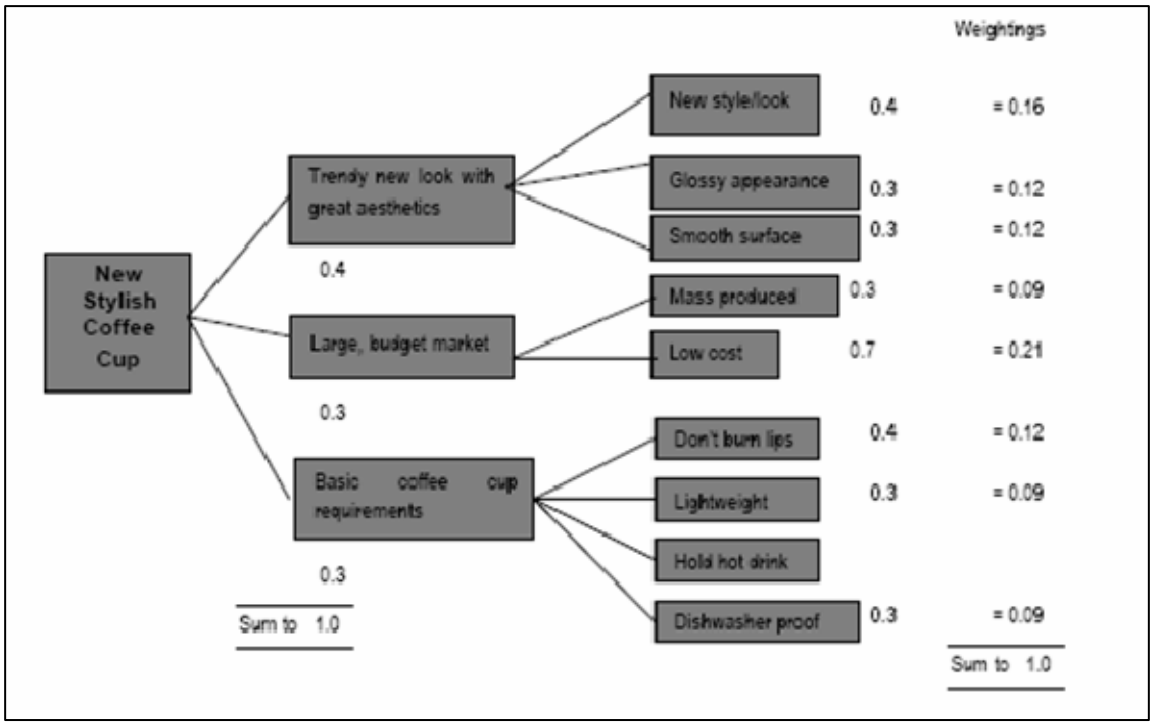


Figure 39. MoE Example (From: Design Methods Fact Sheet)

Engineers use the Measures of Effectiveness to develop engineering specifications. Measures of Performance are used to ensure the system falls within the technical specifications. MoP are quantitative in nature and typically consist of an acceptable range around a desired value. For example, the desired power consumption might be .5 watts. The MoP might say the acceptable power consumption is between .45 watts and .52 watts. Figure 40 is an example of Measures of Performance.

Need or Want	Specification for **New Stylish Coffee Cup**	Page 1
N	Weight < 120g	
W	< 100g	
N	Non porus	
N	Thermal conductivity < 2.5W/m.K	
W	< 1.4 W/m.K	
W	Surface Finish < +- 0.04mm	
N	Produce > 5000 items/ day	
W	> 8000 items/day	
N	Rigid solid @ ~ 110oC	
W	Reflective coating	
W	Volume ~ 280-350ml	

Figure 40. MoP Example (From: Design Methods Fact Sheet)

Although the process and results from developing MoP and MoE appears to be time consuming, they prove extremely useful in developing and analyzing complex systems. As systems become increasingly complex, the design and engineering processes become more difficult. Developing MoP and MoE allows designers to create a product that meets the customers' requirements. Additionally, by developing MoP and MoE, evaluating multiple systems objectively from a qualitative and quantitative perspective is possible.

D. SELECTED MOE AND MOP

The selection of MoE and MoP for this thesis was conducted through market research and analysis of the real-world requirements for deploying an integrated sensor-camera network. Initial MoE were based on the needs of the COASTS 2006 scenario and experiments. Also, civilian law enforcement officers along with military security and force protection officers provided input. The following sections describe the developed MoE and MoP for the specific aspects of the integrated network.

1. Sensors

The sensor aspect of the network was the most scrutinized part of the integrated network because the technology is relatively new. The weighted values were spread almost equally among the broad categories of sensing capabilities, deploy ability, interoperability, and availability. The sensing capability requirements focused primarily on the types of objects they could detect, the range at which objects could be detected, and the types of sensors available. The deploy ability focused primarily on the physical environments in which they could reliably operate the performance under adverse climactic conditions, battery life, and logistics footprint. Interoperability values focused on the ability to work within existing infrastructure. The availability values primarily focused on the COTS aspect along with the ease of configuration. Figure 41 depicts the selected MoE, and Figure 42 illustrates the selected MoP.

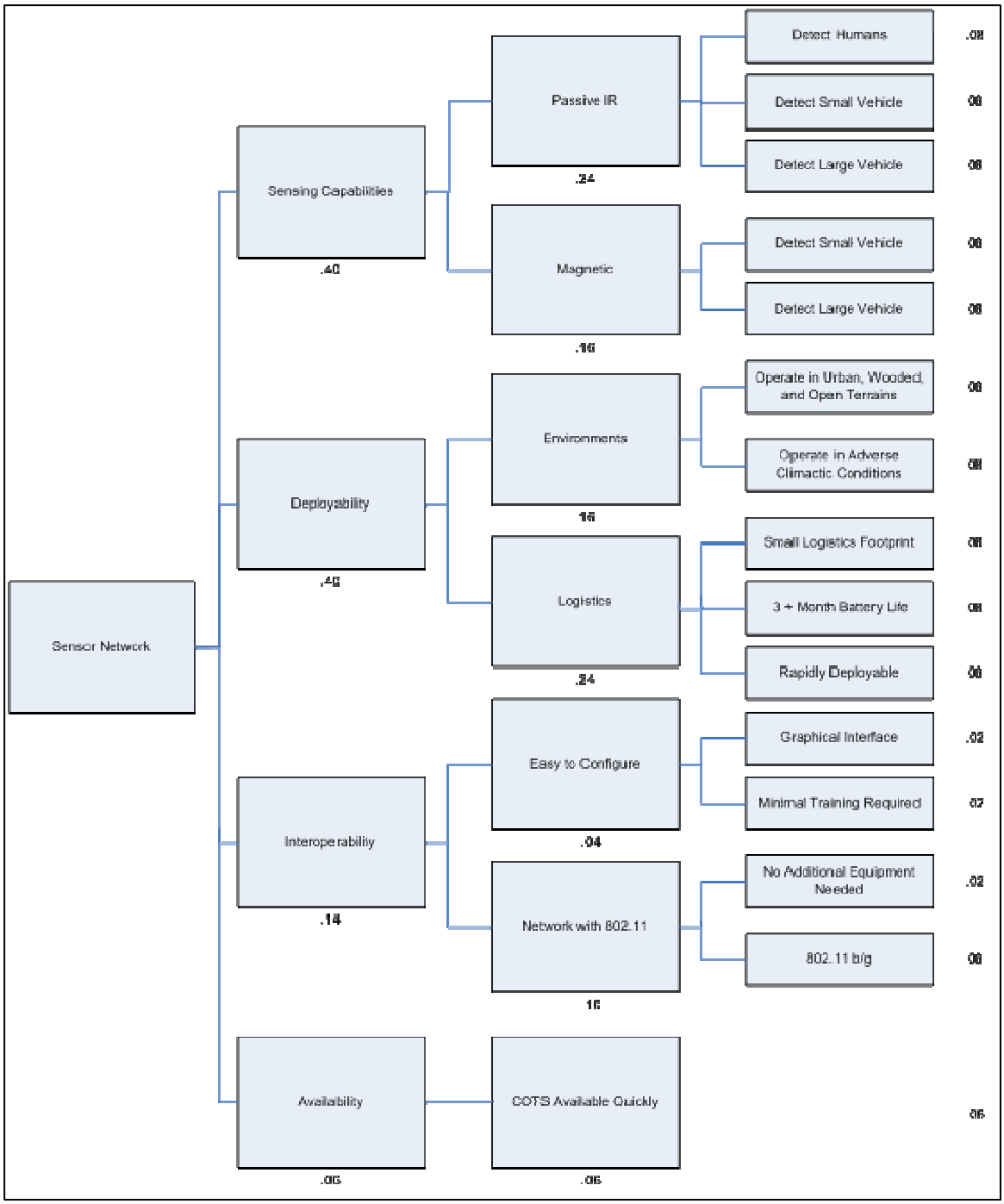


Figure 41. Selected Sensor MoE

NEED/WANT	SPECIFICATION
W	< 10 False Detections per Hour
N	99% Probability of Detection for Humans at 15 Feet
N	99.5% Probability of Detection for Vehicles at 15 Feet
W	Ability to Classify an Object Based on Sensor Values
N	Maximum Detection Range > 30 Feet for Humans
N	Maximum Detection Range > 75 Feet for Vehicles
W	Maximum Communications Range >= 120 Feet
W	Maximum Reassociation Range >= 60 Feet
W	Deployable in 10 Minutes
N	Operate with 802.11 b/g
N	Multiple Sensor Types
N	Battery Life > 3 Months
N	Operate in Urban, Wooded and Open Terrains
N	Small Form Factor (Size)

Figure 42. Selected Sensor MoP

2. Cameras

The cameras' role in the integrated network is to provide real-time visual information to a watch-stander. This offers several key benefits, including visual verification of sensor activity, remote monitoring, and persistent surveillance. By nature, humans rely heavily on visual information. Providing real-time visual information assists decision makers in making accurate and timely decisions. As a result, the MoE and MoP characteristics for the cameras focus primarily on deploy ability, functionality, and interoperability. Deploy ability aspects include logistic footprints, climactic limitations, and power consumption. Functionality values focus on performance requirements such as frame rates, data format, availability of compression, and the ability to pan, tilt, and zoom. Interoperability values focused on the ability to communicate with various existing networking environments. Figures 43 and 44 illustrate the selected MoE and MoP respectively.

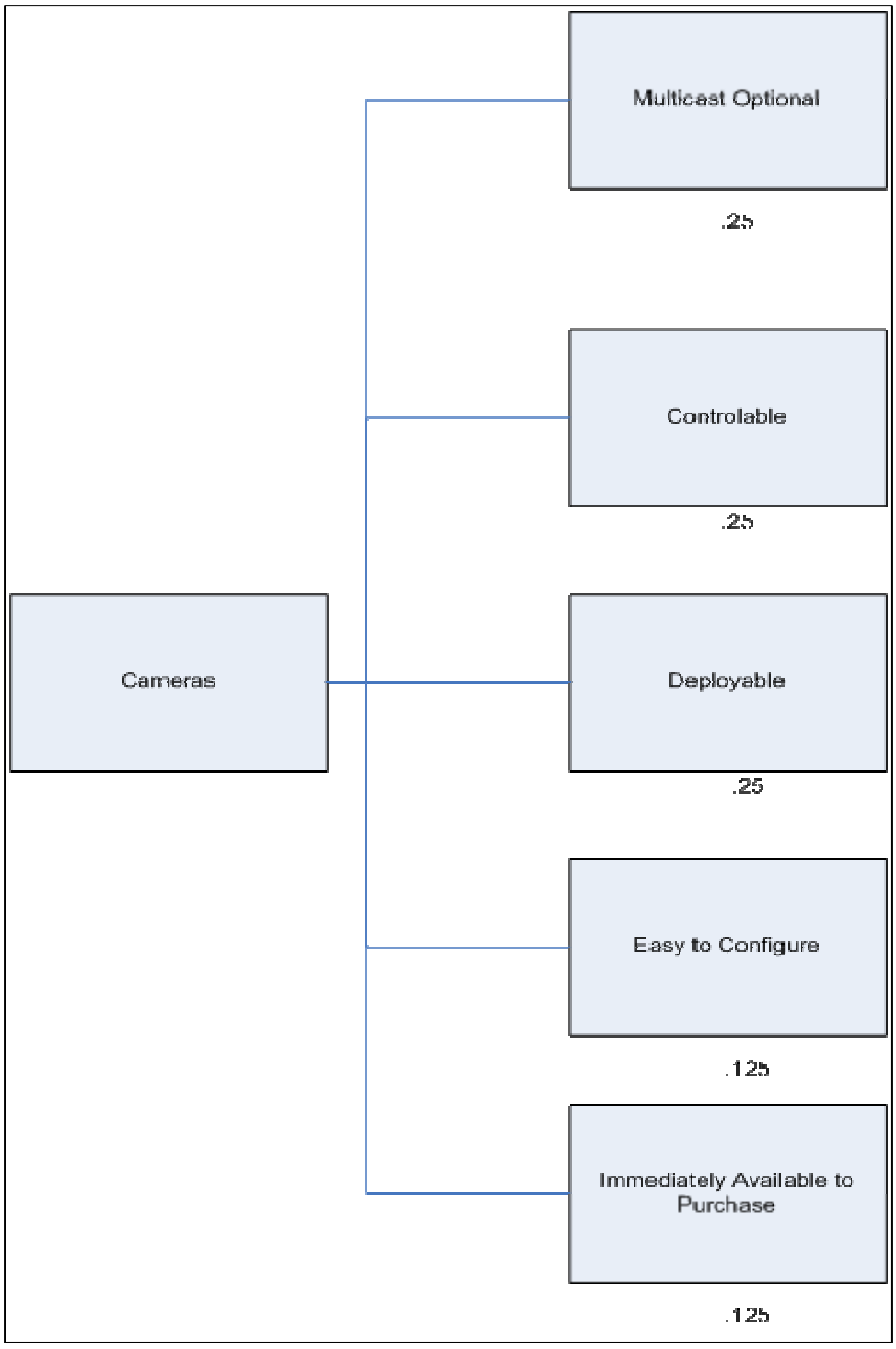


Figure 43. Selected Camera MoE

Need/Want	Specification
W	MPEG Format
N	Multicast Optional
N	Control Pan/Tilt/Zoon
N	IR Illumination
N	20 Frames per Second
N	Wireless Connectivity

Figure 44. Selected Camera MoP

E. EXPERIMENT DESIGN

The testing and evaluation process are intended to ensure that a system meets both the technical specifications and the customer's requirements. During a system's lifecycle, two types of testing exist. The first type of testing is the developmental testing procedure. Developmental testing is done in controlled environments to ensure that the components meet the technical specifications. Developmental testing is typically conducted by the engineer or project manager. Operational testing is the second form of testing. Operational testing is conducted by representative users in real-world, operational scenarios. The goal of operational testing is to measure performance in a broad range of realistic environments (Test and Evaluation Planning Guide). Systems often perform satisfactorily in the statically controlled laboratory conditions but do not perform well in realistic operating environments.

Properly designing the experiments is necessary to infer conclusions from the collected data. Simply employing the system might be an effective proof-of-concept, however, it does not allow analysts to draw conclusions or create models of performance. Experiment design is the structured, organized method to determine the relationship between input factors and the affect they have on the output. It is the strategy of gathering empirical knowledge through the analysis of data gathered during experiments instead of using theoretical models. Designing experiments consists of four steps. The first step is to define the objective of the investigation. The second step is to define the variables that will be controlled during the experiment and the values the variables will have. Ensuring these design variables are measurable and controllable is important. Moreover, the order in which the variables will be changed must be established. The third step in the design of an experiment is to determine response variable. Designers

must ensure that the response variables can be consistently and precisely measured. The final step is to select statistical basis for the experiment. Several statistical models serve as the basis of experiments and ensure that data analysis accurately represents system performance. Two commonly used methods are the full-factor experiment and the Latin hypercube. A full-factor experiment design tests all possible combinations of control variables. Although this method ensures complete analysis of control variables, it often results in an exorbitant number of runs and is often cost prohibitive. Take, for example, a full-factor experiment in which there are ten test parameters with five levels. This experiment would require 5^{10}, or 9,765,625 design points (Bailey et al.).

Latin hypercube sampling is based on Latin square design. It attempts to reduce the number of design points needed for an experiment by ensuring that each value of a variable is represented in a sample. In statistical sampling, a Latin square is a square grid in which each row and column is sampled once and only once. The Latin hypercube is the generalization of this concept to an arbitrary number of dimensions. Essentially, Latin hypercube experimental design significantly reduces the number of design points by creating a statistically representative subset of the full-factor design. The flexibility of the Latin hypercube technique is due to fewer restrictions on the number of factors and levels allowed. Latin hypercube designs are especially well suited for screening factors by analyzing variance techniques and regression analysis. Using a Latin hypercube design, a test of ten parameters with five levels can be reduced to only 37 design points. For experiments in which full-factor testing is unrealistic, the efficiency and flexibility of Latin hypercube design is often the best method to produce statistically reliable results.

Several experiments were designed to evaluate the feasibility of deploying the prototyped sensor-camera network in real-world military and law enforcement scenarios. Each experiment was designed to test specific Measures of Effectiveness and Measures of Performance. The tests focused predominantly on sensor technologies. Five tests were created specifically for the sensors. These consisted of the maximum detection range tests, probability of detection tests, RF break range tests, RF reassociation range tests, and battery life tests. The Latin hypercube design technique is the primary technique used throughout the experiments. Several of the tests had several control

variables each with a large range of values. Conducting full-factor tests would have been time- and cost- prohibitive. The tests were designed to evaluate performance under real-world deployment conditions.

Camera testing designs were less involved. The Axis 213 camera is a commercially available product commonly used in a variety of applications. This camera brings an impressive array of abilities with minimal cost. Additionally, the Axis 213 camera is currently in operation with several law enforcement and military organizations around the world. However, most organizations do not operate in environments as extreme as south-east Asia, Iraq, or Afghanistan. As a result, the testing focused on determining the minimum frame rate need to provide useful video information and on ensuring performance in adverse weather.

Finally, the integrated sensor-camera network was used in several operational scenarios. The scenarios were designed to stress the network design and performance in ways similar to real-world deployments. The operational scenarios were conducted as a part of the broader COASTS 2006 program. A total of four scenarios were conducted throughout the research. The first scenario was conducted in Point Sur, California, during December. This allowed the network to be tested in colder operating environments than could be found around the world. The second scenario testing was done at Fort Hunter Liggett. This scenario allowed the network performance to be tested during moderate environmental conditions. The third and fourth scenarios were conducted in Chiang Mai, Thailand. These scenarios allowed the evaluation of network performance under extreme operating conditions. Temperature and humidity ranges pushed the advertised technical specifications. Temperatures often exceeded 110°F, which is common in war zones such as Iraq and Afghanistan. Conducting operational scenarios over a wide variety of environments allows verifies the models created from testing and also evaluates their performance in realistic deployments.

1. Maximum Detection Range

Maximum detection range tests are designed to determine the maximum range at which the sensor can reliably detect an object. Detection range was measured in feet

from the sensor to the furthest point at which the object could be detected. Because the Crossbow MSP410 motes have both passive infrared sensors and magnetometers, the test was duplicated to focus on each sensing capability individually. Several input variables were identified and defined. These input variables include: sensor elevation, object cross-section, object speed, ambient temperature, pressure, and humidity. Table 7 depicts the input variables, the unit of measurement, and the range of each variable investigated during testing.

VARIABLE	UNIT OF MEASUREMENT	RANGE OF VALUES
Sensor Elevation	Inches (in) above ground level	0 to 12 inches
Object Speed	Miles per hour (mph)	0 to 50 mph
Object Cross Section	Square inches or square feet Three Object types used to simulate traffic	1: Human
		2: Toyota Tacoma
		3: Ford F-250
Air Temperature	Degrees Fahrenheit	30 to 120 F
Atmospheric Pressure	Inches Mercury (inHg)	29 to 32 inHg
Relative Humidity	Percent	5 to 100 %
Time of Day*	Hour	0700 – 2300
NOTE: Since environmental conditions could not be controlled, "Time of Day" was created so tests were done under a variety of conditions. The environmental conditions were recorded for further analysis.		

Table 7. Controlled Variables for Maximum Detection Range Tests

Sensor elevation is hypothesized to affect detection range by raising the sensors above environmental obstacles. Raising the sensors above ground level increases the ability to detect around obstacle such as stones or logs. Additionally, objects such as vehicles and people tend to have more mass above ground level than at ground level. There is, however, a practical limit to sensor elevation. The requirement for covertness prohibits placing a sensor at five feet above ground level. Doing so would make the sensor easily viewable and would allow suspects to avoid the sensor grid. The sensor elevation was limited to one foot above ground level. This allows the sensor to be elevated without making them easily visible. Sensor elevation was measured in inches above ground level.

Object cross-section is hypothesized to affect the detection range by increasing the size of the target. Obviously, detecting a large object is easier than detecting a small object. Increasing the cross-section of the target should increase the range at which the target can be detected. For example, a delivery truck should be more visible than a human simply because the truck takes up more space. Three "classes" of objects were used throughout the experiments that represent the type of objects that would be of interest during operational deployment. The first object class was a human. The person used during the experiment was roughly six feet tall and 180 pounds. The second object used was a small truck. As some tests were conducted in America and others in Thailand, using the same truck in all of the experiments was impossible. However, the trucks used were nearly identical in size. For example, the truck used in America was the Toyota Tacoma Extended Cab. The final class of object was the large truck. The large truck is to simulate a van or truck which might be moving personnel or equipment. The primary vehicle used was the Ford F-250. A twelve-passenger van was also used and produced similar results because it was roughly the same size.

The third input variable was the object speed. Object speed is thought to affect the detection range by reducing the amount of time an object is in the detection area of the sensors. It is hypothesized that the faster an object is moving, the closer it must be to be detected. Since humans cannot travel as quickly as vehicles, the speed for humans was divided into three categories: 0 to 2 miles per hour, 2 to 4 miles per hour, and running (4 to 6 miles per hour). The range of vehicular speeds was from 5 to 50 miles per hour.

The ambient temperature, pressure and humidity are factors that are not controllable in operational testing. Conceptually, the temperature in areas of operation could easily range from 25°F to 150° F. Atmospheric pressure could vary between 29.0 inches mercury and 32.0 inches mercury. Humidity could easily vary from 5% to 100%. Since the environments could not be controlled, they were recorded and used during the analysis process. To ensure that a wide variety of environmental conditions were experienced, the testing was spread over five months and various locations. Additionally, a "time of day" variable was developed in an attempt to further increase the conditions experienced. The variable established sixteen hours during which experiments would be

conducted. The "work day" started at seven o'clock in the morning and was conducted until eleven o'clock at night. This reduced the possibility of inadvertently limiting the environmental conditions by conducting tests at the same time during the day.

Conducting a full-factor test would have resulted in an exorbitant number of design points. Using a spreadsheet program developed by Lieutenant Colonel Thomas Cioppa, a Latin hypercube sample was created. This allowed the experiment to be completed with only 17 design points.

Physically conducting the experiments consisted of several steps. First, the needed equipment was set up. The BS was attached to a laptop running the MOTE-View and Surge View software. Then a mote was activated and the connection to the BS was verified. Next, the sensor was raised to the indicated sensor elevation. Then the object moved toward the sensor until detection was indicated on the software. Doing this indicated the maximum distance the object could be detected. Next, the object moved roughly twenty feet closer to the sensor and turned 90° so that the direction of travel was perpendicular to the sensor. The object would then repeatedly travel perpendicular to the sensor at the indicated speed. If the sensor detected the object, the object moved farther away from the sensor. This process was repeated until the maximum detection range was reached. Finally, all the required information was recorded. This process was completed several times for each design point.

2. Probability of Detection

The probability of detection tests are designed to develop a tool to help network architects custom design a network. Understanding what factors affect the probability of detection and the impact the variables have on the detection probability at various distances assists network planners to ensure they achieve the desired goals. The control variables for the probability test are exactly the same as the variables for the maximum detection range. Exactly the same design points were used. Only two significant differences were introduced. First, was deciding the distances and the intervals for the experiments. After considering possible deployment scenarios and analyzing the RF reassociation ranges, several distances were selected for further analysis. The distances

selected were 10, 15, 20, 30, 40, 50, 60, 70, and 80 feet. These selected distances provided information on common deployment scenarios for perimeter defense, vehicle detection, and dense deployment. The second difference was the number of times the object moved perpendicularly past the sensor. For this experiment, the object would cross the sensor coverage area. Detection or non-detection was recorded. This process was repeated 100 times for each design point. After all the design points were accomplished for a given distance, the entire process was repeated for the next distance.

3. Break Range

Understanding the maximum reliable RF communications range of a network has significant effects on network design. The need to understand the communications break range is compounded by the need for survivability. Since network reliability and survivability often depend on the ability to communicate with multiple nodes, understanding how communications range changes greatly improves one's ability to design a robust and reliable network while maximizing the size of the sensor grid.

Although the complete understanding of RF propagation is not the primary focus of this thesis, the radio range affects network performance and is investigated. A thorough analysis of RF properties at 433 MHz is complex enough to warrant its own thesis. However, general performance is addressed to determine the feasibility of deploying the prototyped network in real-life environments. Several factors are known to affect RF communications range, including terrain, transmission power, receiver sensitivity, RF interference, antenna configurations, elevation, and environmental conditions. Since this thesis focuses on COTS technology, several of these factors could be considered negligible or constant. These tests focus on the effects of transmission elevation and environmental conditions on the break range. To eliminate the effect of terrain, all tests were conducted on a flat road with no objects between the two transmitters. Receiver sensitivity, transmission power, and antenna configuration effects were eliminated by using standard configuration from the manufacturer and ensuring that the transmission powers were all set to the same level. Additionally, the same two nodes were used throughout the tests. Before all tests were conducted, the area was surveyed using a spectrum analyzer to ensure that no other RF activity would interfere. To ensure

exposure to a variety of environmental conditions, a complete round of testing was conducted twice monthly and also in Thailand to allow exposure to extreme heat levels. Table 8 depicts the variables used in the break range tests.

VARIABLE	UNIT OF MEASUREMENT	RANGE OF VALUES
Sensor Elevation	Inches (in) above Ground Level	0 to 12 inches
Terrain	N/A	Flat Road
Transmission Power	Decibels	Standard Configuration from Manufacturer
Receiver Sensitivity	Decibels	Standard Configuration from Manufacturer
RF Interference[1]	Decibels	N/A
Air Temperature	Degrees Fahrenheit	30 to 120 F
Atmospheric Pressure	Inches Mercury (inHg)	29 to 32 inHg
Relative Humidity	Percent	5 to 100 %
Time of Day[2]	Hour	0700 to 2300

NOTES
1. Prior to conducting tests, a spectrum analyzer was used to ensure no RF activity in the frequencies was used by the Crossbow Sensors.
2. Since environmental conditions could not be controlled, "Time of Day" was created so that tests were done under a variety of conditions. The environmental conditions were recorded for further analysis.

Table 8. Break Range Testing Variables

Initial empirical evidence showed that the break range between two motes was different than that of a mote and the base station. As a result, two separate break range tests were conducted. The first break range test was the Mote-Mote break range. The second test was the BS-Mote break range.

The first step of the Mote-Mote testing process was to initialize the components. This involves connecting the BS to the laptop, powering-up the motes, and verifying communication through the Surge View software. Next, the motes were placed at the indicated elevation and set at a distance of ten feet apart. Next, Surge View was checked to verify that the farthest mote was communicating with the closest mote instead of with the base station. After this was verified, the link quality was recorded. The furthest mote was then moved five feet away. Link quality was again recorded. This process was repeated until link quality reached zero and the software indicated the connection was

lost. The environmental data were recorded, concluding one run of the experiment. A total of ten runs were conducted at each elevation. Next, the entire process was repeated at a sensor elevation of six inches and at one foot.

The BS-Mote break-range testing procedures were virtually identical to the Mote-Mote procedures. First, the components were initialized and placed at the indicated elevations. Next the single mote was placed ten feet from the BS. The connection was verified and the link quality was recorded. The mote was then moved five more feet away. This was repeated until the connection was lost. Environmental conditions were recorded and one run of the experiment completed. Again, a total of ten runs were completed for each elevation. The entire process was then repeated at elevations of six inches and at one foot.

4. Reassociation Range

As with the RF break range, understanding the reassociation range of the motes is an important tool for planning a wireless sensor network. The survivability and self-healing characteristics of WSNs are extremely important for tactical deployments. The hostile conditions—such as explosions, sand storms, and enemies tampering with equipment—make the failure of one or more sensor nodes extremely likely. The network must be able to overcome the loss nodes and continue functioning. Understanding how the reassociation range can change is a useful planning tool to ensure the network can self-heal in a timely manner.

The reassociation range tests investigated the same parameters and followed the same constraints as the break-range tests. An additional constraint was placed on the time given for reassociation. In a tactical scenario, timely information is critical. The time for reassociation was limited to ten minutes because it was sufficient to allow the network to heal, but not long enough to present a significant loss in tactical functionality. Table 9 details the variables used in the reassociation range tests. As with the break range, initial observations indicated the reassociation ranges between two motes and a mote and the BS differed, resulting in two reassociation range tests.

VARIABLE	UNIT OF MEASUREMENT	RANGE OF VALUES
Sensor Elevation	Inches (in) above Ground Level	0 to 12 inches
Terrain	N/A	Flat Road
Transmission Power	Decibels	Standard Configuration from Manufacturer
Receiver Sensitivity	Decibels	Standard Configuration from Manufacturer
Time to Reaassociate	Minutes	0 to 10 minutes
RF Interference[1]	Decibels	N/A
Air Temperature	Degrees Fahrenheit	30 to 120 F
Atmospheric Pressure	Inches Mercury (inHg)	29 to 32 inHg
Relative Humidity	Percent	5 to 100 %
Time of Day[2]	Hour	0700 to 2300

NOTES
1. Prior to conducting tests, a spectrum analyzer was used to ensure no RF activity in the frequencies was used by the Crossbow Sensors.
2. Since environmental conditions could not be controlled, "Time of Day" was created so tests were done under a variety of conditions. The environmental conditions were recorded for further analysis.

Table 9. Break Range Testing Variables

The tests relied on initial analysis of the break-range tests to estimate how far the nodes would need to be stretched apart before the link was lost. First, the components were initialized and the connection verified. The farthest mote was iteratively stretched until the RF link was lost. The mote was then moved five feet closer to the other mote or BS. If the connection was re-established within ten minutes, the distance was recorded as the reassociation range. If the connection was not restored, the mote was moved back to the original starting position. The nodes were then stretched apart until the link was lost again. The mote was moved an additional five feet closer. This process was repeated until the reassociation range was established. The entire process was repeated ten times at each sensor elevation.

5. Battery Life

The battery life of the nodes in the integrated network determines the effective on-station time. Long stand-alone on-station times are required to achieve the Expeditionary Sensor Grid (ESG) envisioned by Sea Power 21 and Joint Vision 2020. From a network management point-of-view, the number of nodes needed to form large, densely populated sensor grids also encourages long battery life. For example, replacing

the power source on 15,000 sensors every two days is not only economically unfeasible, but it also man-power intensive. From a tactical point-of-view, long on-station time is a requirement. The network must be rapidly deployable and need no on-site interaction for extended periods of time. Returning to replace power sources will alert the enemy of the location of the sensors. The enemy will then simply avoid the sensor grid, rendering it tactically useless. In an environment such as Afghanistan, Iraq, or Thailand, insurgents might place snipers near the nodes to deter anyone replacing a power source.

The factors that are known to affect power consumption in sensor networks were discussed in Chapter II. However, the objective of this test is not to determine the factors that affect power consumption. Nor was the objective to establish the effect of changing a parameter on battery life. The objective was to discover the on-station time that can be expected from an unchanged system from the manufacturers.

Two constraints were used on the test. The first constraint was that the BS was powered from a wall socket, essentially giving the BS an indefinite power supply. This was considered acceptable because the objective of the test focused on the sensor nodes. However, failure of the BS would prohibit the Crossbow sensors from communicating with an external network, therefore, rendering it ineffective. The second constraint was the network was considered ineffective once six of the eight sensors died. Although data feeds from two sensors are better than no sensor data at all, two sensors would not be able to represent the sensor grid sufficiently. For example, if a network designed for perimeter defense lost 75 percent of the sensors, it would not provide adequate coverage. Large coverage gaps would render the network tactically useless.

The testing procedure for the battery life test is straight forward. Fresh AA batteries were placed in each of the eight motes from the Crossbow MSP410 set. The BS was connected to a laptop running MOTE-View and the motes were turned on and placed in an environment with a moderate amount of traffic. The motes were allowed to run until six of the eight consumed the power source. The elapsed time is recorded as the battery life (or on-station time) of the network. This process was conducted ten times.

F. GENERAL OBSERVATIONS

The tests mentioned above were carefully designed to produce results that could be considered statistically representative of performance. The results can be the basis for determining the feasibility of deploying the network in military and law enforcement applications. However, several other characteristics are of general interest in evaluating network performance and design. Although no experiments were designed to test these characteristics directly, they were observed numerous times in a variety of environmental conditions and operational scenarios.

The first observed characteristic was performance in three common operating environments. The three environments were chosen because they are commonly visited by military and law enforcement forces. The first environment observed was an "open" environment such as a field or a road. All of the tests described previously were conducted in an open environment. This environment is commonly encountered in perimeter defense and object tracking applications. The second environment was the urban environment. The urban environment would most commonly be encountered by law enforcement agencies. An integrated sensor-camera network can also be employed by military forces in urban environments such as Baghdad, Iraq. The final environment observed was the wooded environment. A sensor-camera network might commonly be deployed in a wooded environment for perimeter defense, environmental monitoring, and even "smart obstacle" scenarios. Understanding how the network performs in these environments is useful in planning, deploying, and evaluating the network.

The second observation was the effect of deploying the network in uneven environments. All of the tests were conducted on flat ground. Realistically, the network will be deployed on hills, in ravines, and on uneven ground. Having a general idea of how the network will perform in such environments is also useful in evaluating the network.

The final general observation is the effect of rain on performance. A sensor-camera network will be deployed in places that undergo the gamut of weather phenomenon. It is important that the network be able to perform satisfactorily in all conditions. Rain will not stop an enemy from attacking and must not significantly

degrade network performance. Since it was impossible to control rain for testing purposes, performance in rain was observed on several occasions. The performance objectives were to determine the effect on detection and communication ranges.

This chapter introduced and discussed the processes of testing and evaluating a system during the development phase. Thorough testing and evaluating systems is a critical component during the system's lifecycle. The attributes of an effective metric, measures of effectiveness, and measures of performance were introduced. The metrics, MoP and MoE used to evaluate the integrated sensor-camera were described. The specific tests and processes were described in detail. Finally, this chapter concluded by describing general performance characteristics that will be used to help develop, plan, and test an integrated sensor-camera network.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. ANALYSIS OF EXPERIMENT RESULTS

This chapter discusses the results from the experiments designed to evaluate the performance of the integrated sensor-camera network described in Chapter V. All tests were conducted according to the process described in Chapter IV. The experiments are categorized into detection ranges, probability of detection, communication ranges, battery life, and general observations.

A. DETECTION RANGE TESTS

The sensor subsystem of the Crossbow MSP410CA Wireless Security Mote Kit was tested in depth. The objective of the detection range tests was to determine the maximum range at which the sensor can reliably detect an object. Furthermore, a Latin hypercube design was used to create a model for predicting the maximum detection range based on sensor elevation, object cross-section, object speed, ambient temperature, pressure, and humidity. Because the sensing subsystem contains multiple sensors, the tests were repeated for both the PIR sensor and for the magnetometer. The results are discussed in detail in the following sections.

1. PIR Detection Range Results

The PIR sensor subsystem was tested against objects ranging from personnel to large trucks. Tests were conducted under a variety of object speeds, sensor elevations, and weather conditions. Successful tests indicate the maximum detection range for a human of 45 feet and a maximum detection range of large trucks of 148 feet. The results of the experiments are shown in Tables 10 and 11.

Detection Distance (Feet)	Elevation (Inches)	Speed[1]	Time of Day[2]	Temperature (F)	Pressure (inHg)	Humidity
45.3	12	3	6	64.9	30.15	53.3
27.9	3	3	9	75.1	29.76	70.6
35.7	5	1	4	70.6	30.15	33.4
38.4	8	2	16	77	29.97	94.9
42.1	11	2	2	59.3	30.2	51.4
32.6	4	2	13	57.4	30.00	94.1
28.1	2	3	5	54.5	30.12	82.8
35.2	11	3	15	100.7	29.6	23.9
38.5	6	2	8	88	29.80	77.2
25.6	0	1	10	64.9	30.15	53.3
31.4	9	1	7	106.8	29.57	20.3
39.5	7	3	12	41.8	29.62	95.1
38.1	5	2	0	36.4	28.68	93.6
26.2	1	2	14	93.6	29.74	46.7
37.7	8	2	3	81.4	29.88	84.2
39.3	10	1	11	57.6	29.56	85.5
27.5	2	2	1	61.5	29.85	83.6

Note:

1. Speed categories are defined as follows: 1 represents 0 to 2 mph, 2 represents 2 to 4 mph, 3 represents 4 to 6 mph.
2. "Time of Day" was created so tests were done under a variety of weather conditions.

Table 10. PIR Detection Range Results for a Human

Once collected, the data were analyzed using linear regression and Analysis of Variance (ANOVA) techniques. The initial analysis resulted in the following relationship:

Human PIR Detection Range = 8.5 + (1.47 x Sensor Elevation) – (0.357 x Speed) – (0.0828 x Temperature) + (0.70 x Pressure) + (0.0402 x Humidity).

Furthermore, ANOVA analysis shows that the sensor elevation and ambient temperature are the two most significant predictors of the detection range. Of the investigated predictors, sensor elevation and temperature had the most statistically significant impact on the detection range. Given a ten-percent significance level, the equation can be simplified to:

Human PIR Detection Range = 33.8 + (1.42 x Sensor Elevation) – (0.0828 x Temperature).

This result corroborates expectations. Raising the sensor from the ground prevents obstruction from environmental obstacles and brings the sensor closer to the center of mass of the human, which will increase the likelihood the object is detected. Due to the nature of the PIR sensor in the motes, the ambient temperature also is expected to impact the detection capabilities. As the temperature increases, the PIR sensor cannot easily distinguish between the heat emitted by an object and the ambient heat emitted by the surrounding environment.

Detection Distance (Feet)	Sensor Elevation (Inches)	Cross Section[1]	Speed (MPH)	Time of Day[2]	Temperature (F)	Pressure (inHg)	Humidity (%)
150.6	12	3	19	6	64.9	30.15	53.3
86.2	3	3	8	9	75.1	29.76	70.6
79.2	5	1	11	4	70.6	30.15	33.4
110.8	8	2	13	16	77	29.97	94.9
124.1	11	2	39	2	59.3	30.2	51.4
93.8	4	2	50	13	57.4	30.00	94.1
109.0	2	3	33	5	54.5	30.12	82.8
143.6	11	3	30	15	100.7	29.6	23.9
104.0	6	2	28	8	88	29.80	77.2
72.1	0	1	36	10	64.9	30.15	53.3
86.4	9	1	47	7	106.8	29.57	20.3
100.5	7	3	44	12	41.8	29.62	95.1
101.4	5	2	42	0	36.4	28.68	93.6
80.6	1	2	16	14	93.6	29.74	46.7
102.4	8	2	5	3	81.4	29.88	84.2
73.7	10	1	22	11	57.6	29.56	85.5
60.3	2	2	25	1	61.5	29.85	83.6

Note:
1. Cross Section values are categorical. 1 represents a small car, 2 represents a small truck, 3 represents a large truck.
2. "Time of Day" was created so tests were done under a variety of weather conditions.

Table 11. PIR Vehicle Detection Range Results

The data analysis for vehicle detection using the PIR sensor was conducted in the same manner as for human detection. The resulting equation for vehicle detection, shown below, again confirmed expectations that sensor elevation and object cross section have the most significant impact on detection capabilities.

Vehicle Detection Range = -185 + (3.75 x Sensor Elevation) + (19.3 x Cross Section) + (0.178 x Speed) – (0.019 x Temperature) + (7.6 x Pressure) – (0.149 x Humidity).

However, ANOVA analysis shows that the speed, temperature, pressure, and humidity predictors were not statistically significant. Assuming a ten-percent significance level, the above equation can be reduced to:

Vehicle Detection Range = 37.7 + (3.94 x Sensor Elevation) + (18.0 x Cross Section).

The resulting equation appears to support the data provided by Crossbow, which claims that PIR performance is dependent upon ambient environmental conditions, velocity, and the size of the object. Experiments showed the most dominant predictors of vehicle detection range are sensor elevation and the cross section of the vehicle. One would expect that object speed is a statistically significant determinant of detection range. However, ANOVA analysis showed that object speed was not significant at the ten-percent level. This result was collaborated by follow-up tests, which showed that the detection range with the object traveling 5 mph was nearly identical to the detection range of the object traveling 65 mph.

2. Magnetometer Detection Range Results

As with the PIR subsystem, the magnetometer tests were designed to determine the maximum detection range based on object cross sections, object speeds, sensor elevations, and weather conditions. Conceptually, a magnetic detection can be used to classify an object detected by a sensor grid. As a result, the ability to model detection range is also important. Magnetic detection range tests were conducted using the same three vehicles used in the PIR detection range tests. Successful tests indicate detection of a large truck at 58 feet, a small truck at 45 feet, and a car at 32 feet. Table 12 presents the results of magnetic detection range experiments.

Detection Distance (Feet)	Sensor Elevation (Inches)	Cross Section[1]	Speed (MPH)	Time of Day[2]	Temperature (F)	Pressure (inHg)	Humidity (%)
58.9	12	3	19	6	64.9	30.15	53.3
52.4	3	3	8	9	75.1	29.76	70.6
31.2	5	1	11	4	70.6	30.15	33.4
43.9	8	2	13	16	77	29.97	94.9
45.3	11	2	39	2	59.3	30.2	51.4
42.7	4	2	50	13	57.4	30.00	94.1
51.7	2	3	33	5	54.5	30.12	82.8
58.2	11	3	30	15	100.7	29.6	23.9
43.2	6	2	28	8	88	29.80	77.2
31.9	0	1	36	10	64.9	30.15	53.3
31.9	9	1	47	7	106.8	29.57	20.3
56.1	7	3	44	12	41.8	29.62	95.1
42.9	5	2	42	0	36.4	28.68	93.6
41.0	1	2	16	14	93.6	29.74	46.7
43.4	8	2	5	3	81.4	29.88	84.2
32.4	10	1	22	11	57.6	29.56	85.5
41.9	2	2	25	1	61.5	29.85	83.6

Note:

1. Cross Section values are categorical. 1 represents a small car, 2 represents a small truck, 3 represents a large truck.
2. "Time of Day" was created so tests were done under a variety of weather conditions.

Table 12. Magnetometer Detection Rang Results

The magnetometer detection range results were analyzed using the same ANOVA and regression analysis techniques. Analysis produced the following prediction equation:

Magnetic Detection Range = 5.5 + (0.404 x Sensor Elevation) + (11.7 x Cross Section) + (0.0136 x Speed) – (0.0200 x Temperature) + (.482 x Pressure) – (0.0136 x Humidity).

The equation can be simplified upon further review. Only sensor elevation and cross section are significant at the ten-percent level. The equation produced, combined with ANOVA analysis, confirm that the most significant determinant in the magnetic detection range is the cross section of the vehicle. Larger vehicles often contain more metallic parts, increasing the distance that the sensor can detect an object. The analysis shows that the magnetic detection ranges can be predicted based upon the following equation:

Magnetic Detection Range = 17.6 + (0.415 x Sensor Elevation)+ (11.6 x Cross Section).

The various detection range results supported the original hypotheses and technical information provided by Crossbow. As expected, sensor elevation has a significant positive relationship with detection distances. Additionally, the size and physical composition of the object significantly impact the maximum detection distance. The sensor subsystem met or exceeded the selected MoE and MoP concerning maximum detection ranges. The maximum detection range for humans during the experiments was consistently over 30 feet. The MoP set a minimum threshold for human detection at 30 feet. Likewise, vehicle detection far exceeded the 75 foot threshold established by the MoP. The PIR sensor was able to detect small vehicles well over 80 feet and consistently detected vehicles at distances over 105 feet. These values also exceeded the values published by Crossbow in technical documentation. Additionally, the magnetometer could to detect vehicles at over 40 feet. This shows that the PIR and magnetic sensors can be used to distinguish between human and vehicular traffic easily. However, for both PIR and magnetometer detection range results, there appears to be an absolute maximum detection range at which raising the sensor elevation will not increase performance. For example, the PIR sensor never detected a human at ranges over 48 feet, regardless of the sensor's elevation. These limits are determined by the sensitivity and nature of the sensor subsystems.

B. PROBABILITY OF DETECTION RESULTS

Understanding how network parameters affect the probability of detection is an important ability during sensor network planning. The probability of detection experiments were designed to provide network engineers a tool to help design a network to meet the intended needs properly. Tests were conducted at specified intervals using the same design points as the detection range tests. Each design point was repeated 100 times to produce a probability value for each design point. The complete results of the experiments can be found in Appendix B. At each specified distance, the design points were analyzed using linear regression to create a prediction equation. The final equations are shown below:

$$P_{d\ 10\ Feet} = 0.974 + (0.000615 \times \text{Sensor Elevation}) + (0.00723 \times \text{Cross Section})$$

$$P_{d\ 15\ Feet} = 0.967 + (0.000663 \times \text{Sensor Elevation}) + (0.00957 \times \text{Cross Section})$$

$$P_{d\ 20\ Feet} = 0.967 + (0.00143 \times \text{Sensor Elevation}) + (0.00705 \times \text{Cross Section})$$

$$P_{d\ 30\ Feet} = 0.964 + (0.00178 \times \text{Sensor Elevation}) + (0.0060 \times \text{Cross Section})$$

$$P_{d\ 40\ Feet} = 0.959 + (0.00123 \times \text{Sensor Elevation}) + (0.00525 \times \text{Cross Section})$$

$$P_{d\ 50\ Feet} = 0.907 + (0.002277 \times \text{Sensor Elevation}) + (0.00889 \times \text{Cross Section})$$

$$P_{d\ 60\ Feet} = 0.908 + (0.00175 \times \text{Sensor Elevation}) + (0.00931 \times \text{Cross Section})$$

$$P_{d\ 70\ Feet} = 0.893 + (0.00204 \times \text{Sensor Elevation}) + (0.0104 \times \text{Cross Section})$$

$$P_{d\ 80\ Feet} = 0.893 + (0.00204 \times \text{Sensor Elevation}) + (0.0104 \times \text{Cross Section}).$$

The results from the probability of detection experiments again confirmed the initial theory that sensor elevation and object cross section have the most significant impact on the probability of detection. This was observed during the experiments and confirmed after linear regression and ANOVA analysis. As the distance from the sensor increased, the equation's constant decreased, which indicates the overall probability of detection is decreasing. At the same time the coefficients for the predictors became larger, indicating the sensor's elevation and the object's cross section were impacting the probability of detection more noticeably. At large distances, the object's cross section became the most significant predictor. This fact validates the theory that larger objects are more easily detected at long distances.

C. BREAK RANGE RESULTS

The self-healing nature of sensor networks requires the nodes to be capable of communicating with multiple other nodes. As a result, understanding the maximum communications distance is a useful tool for planning sensor-camera networks. The break range tests were designed to discover the relationship between maximum communications distances and various determinants such as sensor elevation and environmental conditions. The break range tests were conducted with sensor elevations

at ground level, six inches, and one foot above ground level. Additionally, all tests were conducted on flat asphalt roads to reduce any terrain interference. The following sections describe the results for mote-to-mote and mote-to-base station experiments.

1. Mote-to-Mote Break Range Results

Empirical evidence showed that Mote-to-Mote communication distances were farther than Mote-to-Base Station distances. Table 13 shows the average result for each elevation. The complete results can be found in Appendix B. Mote-to-Mote communication distances increased significantly as sensor elevation increased. Furthermore, regression analysis showed that the environmental conditions do not have a statistically significant affect on the communications distance. However, communication distances fell significantly during rain showers. Experiments were not conducted when it was raining. The prediction equation shows the following relationship:

Mote-to-Mote Break Range = 72.7 + (5.19 x Elevation).

Elevation	Distance	Temperature	Pressure	Humidity
0	75.30	69.82	29.66	66.27
6	98.75	70.58	29.81	65.87
12	137.60	73.69	29.95	61.54

Table 13. Average Mote-to-Mote Break Range Results

These results confirm the expectations that the most significant determinant of communications distance is sensor elevation. Elevation is known to have a significant impact on line-of-sight transmission distance. Raising the transmission elevation reduces scattering, absorption, and interference from the environment. One would expect that humidity and transmission distance are inversely related. As the moisture level in the air increases RF scattering and absorption should also increase. Surprisingly, the humidity level did not have a significant impact on transmission distance. Although the experimental results fall well short of the advertised communications distance, the maximum mote-to-mote communications distance is acceptable based on the detection ranges. Even at ground level, the break range was greater than most maximum detection

ranges. However, it is important to note that the break range is the maximum range achieved. Networks nodes should be placed within the reassociation range to increase reliability and survivability.

2. Mote-to-Base Station Break Range Results

The Mote-to-Base Station experiments were designed to help determine how far the sensor nodes can be placed from the base station and still communicate with it. Understanding the Mote-to-Base Station break range is important because multiple nodes must be able to communicate directly to the base station to ensure the survivability of the network. The experiments were conducted in the same manner as the mote-to-mote experiments.

The mote-to-base station break range results were typically 10 to 20 percent shorter than the mote-to-mote results. The exact reasons for these differences are not known, but it is hypothesized that the BS's responsibilities result in lower effective transmission power. Table 14 shows the average result for each elevation. The complete results can be found in Appendix B.

Elevation	Distance	Temperature	Pressure	Humidity
0	52.1	70.95	29.77	65.59
6	89.2	73.21	29.95	66.23
12	115.75	72.55	29.70	63.47

Table 14. Average Mote-to-BS Break Range Results

The results of the mote-to-base station test results again confirmed that elevation was the most statistically significant determinant of the break range. Regression analysis showed that there are two significant inputs based on the following relationships:

Mote-to-Base Station Break Range = 60.1 + (5.29 x Elevation) – (0.0944 x Humidity).

The first statistically significant variable is the elevation. Additionally, the mote-to-base station break range results indicated that humidity was statistically significant.

The analysis showed that humidity and break range are negatively correlated. As the humidity increases, the break range decreases. This supports existing research, which shows that low frequency RF communications are slightly degraded as humidity increases.

The break range results satisfied the specified MoE and MOP. Though the communication ranges at ground level were not excellent, performance increased significantly as the mote's elevation increased. The best performance from both the sensing and communications points of view occurred at one foot elevation. From a tactical perspective, a one-foot elevation is acceptable because it significantly increases performance but does not reduce any covertness.

D. REASSOCIATION RANGE RESULTS

Understanding the reassociation range of the sensor network is an important part of evaluating and designing an integrated sensor-camera network. The inherent applications of a sensor-camera network require redundant communications paths and the ability to self-heal. As with the break range experiments, initial evidence showed that the reassociation range differed for mote-to-mote and mote-to-base station scenarios. The following sections describe the results for both scenarios.

1. Mote-to-Mote Reassociation Range Results

Like the break range results, the mote-to-mote reassociation results were farther than the mote-to-base station results. The same control variables were used for the reassociation experiments. Table 15 summarizes the average results the mote-to-mote tests. The complete results can be found in Appendix B.

Elevation	Distance	Temperature	Pressure	Humidity
0	45.25	71.53	29.64	66.02
6	51.5	68.93	29.80	65.87
12	63.8	73.64	29.99	61.79

Table 15. Mote-to-Mote Reassociation Range Results

After applying linear regression techniques to the data, the following relationship was discovered:

Mote-to-Mote Reassociation Range = 48.1 + (1.52 x Elevation) – (0.0569 x Humidity).

The resulting prediction equation again contains two significant inputs. The equation again supported the hypothesis that elevation significantly impacts the reassociation range. It further showed the small negative correlation between humidity and transmission ranges.

2. Mote-to-Base Station Reassociation Range Results

The mote-to-base station reassociation ranges were slightly shorter than the mote-to-mote results. The exact cause of the difference is not known, but it is hypothesized that the roles and responsibilities of the base station reduce the available energy and time for reassociation. The average results for the mote-to-base station results are summarized in Table 16 and the complete results can be found in Appendix B.

Elevation	Distance	Temperature	Pressure	Humidity
0	37.5	71.52	29.84	63.09
6	47.1	70.62	29.75	65.61
12	54.66	71.95	29.84	64.98

Table 16. Mote-to-Base Station Reassociation Range Results

Linear regression analysis yielded a prediction equation with two statistically significant inputs. The first input is elevation, which has a strong positive correlation with reassociation range. This relationship is expected, especially given the results of all

the other experiments. The second significant predictor is humidity, which is weakly and negatively correlated. The final prediction equation is as follows:

Reassociation Range = 41.1 + (1.44 x Elevation) – (0.0516 x Humidity).

From an operational perspective, the mote-to-base station reassociation range results are lacking. The results indicate that the Crossbow sensor suite does not provide the needed range to satisfy the MoP and MoE. This might be due in part to the time limit applied to the experiment. Possibly, the results might be significantly farther, given no time constraints. However, the time constraints used are acceptable, given the time sensitive constraints of tactical military and law enforcement applications.

E. BATTERY LIFE RESULTS

The battery life directly influences the feasibility of deploying a sensor-camera grid in military and law enforcement applications. To be truly effective, the network must have long on-station times with minimal human interaction or monitoring. The battery life tests showed that the average expected on-station time for the prototyped network is 90 hours or 3.75 days. The maximum battery life achieved during the tests was 4.5 days while the shortest battery life was 1.9 days. The variation in lifetime is explained by the inability to control the traffic surrounding the testing area. During times of heavy traffic, the nodes report detections more frequently. The increase in transmission significantly increases power consumption and, therefore, lowers battery life.

The battery life tests clearly show the prototyped network is not suitable for most military and law enforcement applications. The MoP and MoE call for a minimum on-station time of three months, with six months to one year desirable. The prototyped network falls significantly short of the desired performance. The battery life tests show that the designed network is not appropriate for applications requiring long on-station times. However, the network is well suited for applications that require short on-station times. For example, the prototyped sensor-camera network is well suited for law enforcement perimeter protection scenarios because they are typically short lived.

F. GENERAL OBSERVATIONS

Several general performance characteristics were observed to help evaluate the prototyped network yet were not directly scientifically tested. These general observations focus on the impact of the operational environment, terrain, and rain. Understanding how these factors affect network performance assists in determining the feasibility of deploying the network for military and law enforcement applications.

The first observed characteristic was performance in open, wooded, and urban environments. In open environments, the performance was nearly identical to the performance established during the tests described above. The radio ranges and detection ranges were the greatest in an open environment. The second environment was the wooded environment. Performance in the wooded environment degraded slightly due to interference from trees and shrubs. Maximum radio ranges decreased by roughly 10 to 15 feet. However, the sensor grid was able to cover roughly the same total area due to the ability to cluster and rout message traffic effectively. Detection ranges decreased by roughly five to ten feet due to more interference by the terrain. As expected, as the wooded environment became denser, performance degraded significantly. The final operating environment was the urban terrain. Radio range results decreased by 20 to 30 feet due to the prevalence of energy-diffusing objects, such as vehicles, buildings and RF interference. Likewise, detection ranges also decreased significantly. Also, the number of false detections significantly increased in the urban environment.

The second general performance characteristic observed was the effect of deploying the network in uneven environments such as hills and valleys. The maximum communication ranges appeared to be negatively affected by deploying the network in such an environment. Evidence shows that a three-foot vertical off-set in sensors reduced the maximum communication distance by five to ten feet. Detection ranges were not noticeably affected. If a network is deployed on uneven ground, it must be carefully designed to ensure that there are no unacceptable lapses in detection or communication abilities.

The final general performance observed was the effect of rain on the network. Rain has a significant negative impact on the communication distances of the prototyped

network. Mist and light rain had little or no noticeable affect on performance. However, during periods of heavy rain and downpours communication ranges significantly declined. During several episodes, the communications distance fell by 90 percent. Such drastic declines in communication ranges render the network ineffective.

This chapter presented the results of the various experiments conducted as part of the evaluation process. Additionally, the experiments produced prediction equations to assist network planners in designing an integrated sensor-camera network. First, the maximum detection range experiments were discussed. The analysis covered PIR and magnetometer test results for personnel and vehicles. Next, the probabilities of detection experiments were discussed. Prediction equations were produced to discover how the probability of detection changes based on various inputs at specified object distances. Then the chapter focused on analyzing the maximum break ranges and reassociation ranges. Finally, the chapter concluded with analyzing several of the general observations discussed concerning network performance.

VII. CONCLUSIONS

A. RESEARCH SUMMARY

This thesis focused on testing and evaluating a prototyped integrated sensor-camera network for use in tactical military and law enforcement scenarios. First, the individual technologies were researched and introduced. Chapter II provided an in-depth introduction and discussion of wireless sensor networks. That chapter introduced the technological history of sensor networks and covered current and potential applications of wireless sensor networks. Next, the chapter introduced the leading network architectures and routing techniques. Finally, Chapter II introduced the most common protocols, including IEEE 802.15.4 and ZigBee. Chapter III provided an introduction to digital video technologies. That chapter introduced the process behind capturing, storing, and transmitting digital video data. Next, Chapter III discussed the data rate considerations and introduced the need for effective compression to allow digital video to be transmitted using wireless networking. Finally, Chapter III introduced and briefly described the two leading video compression techniques.

Chapter IV provided an in depth description of the prototyped integrated sensor-camera network. First, that chapter provided an introduction to the COASTS 2006 research project and described the network's role in the COASTS scenario. Next, Chapter IV introduced the specific components used in the network. First, the Crossbow MSP410CA Wireless Security Mote Kit was discussed in depth. Next, the Axis 213 PTZ network camera was introduced as the video component of the network. Finally, Chapter IV described the various other components used to integrate the sensor and camera components with the COASTS wireless network.

Chapter V described the selection of metrics and experiment design processes. First, the chapter introduced the attributes of effective metrics, measures of effectiveness, and measures of performance. Next, the selected measure of effectiveness and measures of performance were described. Finally, the chapter described the experiments used to provide a thorough analysis of the system's actual capabilities in a real-world environment. The experiments were created to allow statistically sound and accurate

results to be drawn from the collected data. The tests focused primarily on the capabilities of the sensors used as part of the prototyped network. They investigated the passive infrared and magnetometer detection ranges, probabilities of detection, RF break ranges, reassociation ranges, and battery life. Understanding the network's capabilities in these areas provides a basis for determining the feasibility of deploying the network for military or law enforcement applications.

Finally, Chapter VI analyzed the results of the experiments. ANOVA and linear regression techniques were applied to produce prediction equations. The prediction equations were intended to serve as a development tool for network planners. Lastly, the chapter briefly compared the results to the selected MoE and MoP. The next sections discuss lessons learned during the process and evaluate the prototyped system.

B. LESSONS LEARNED

Several important lessons were learned during the experimentation process. Many of the lessons learned were the result of actions or difficulties that could not be controlled. Other lessons learned were oversights or challenges that might have been avoidable given additional time and resources.

The first lesson learned during the testing and scenario demonstration processes was the importance and difficulty of power management. The challenge of power management was discussed previously regarding wireless sensor networks. The challenge became evident when deploying in a real-world operational scenario. Although the individual motes lasted significantly longer than expected based on Crossbow technical information, they fell well short of the needed three to six months. Moreover, finding a long lasting power source for the base station proved to be difficult. It is important to choose a system that requires common voltages or can be powered using power sources that are easily available. For example, during the March COASTS demonstration, the Crossbow base station was powered using an improvised source built using AA batteries and electrical tape. A better solution was found for the May

demonstration, but the average battery life was only 1.5 days. Certainly, powering systems in an operational environment is challenging; however, careful planning can ease the challenge significantly.

The second lessoned learned is the burden of heat reduction in an operational environment. Temperature is often referred to as the enemy of electronics. The March and May COASTS demonstrations proved that effective heat reduction and management is an essential aspect in using COTS technology in military applications. Several of the components used in the prototyped network suffered from heat-related malfunctions. For example, the Axis 213 camera is only rated for use up to 104° Fahrenheit. During the March COASTS demonstration in Thailand, the temperature exceeded that mark nearly every day. As a result, the camera would often over heat and shut down. No damage was done to the camera, but the crucial video surveillance capability was lost until the camera cooled down enough to begin normal operations. Research was done to find methods to cool the camera efficiently enough to allow full operation at temperatures above 104° Fahrenheit. The information can be found in Appendix C. After implementing the design recommendations, the camera operated in temperatures exceeding 104° Fahrenheit. In addition to the cameras, the Vlinx Wireless Serial Servers suffered from similar heat-related problems. The Vlinx would typically function well until it overheated and communications were lost. After it overheated, communications were intermittent until the next morning when the server cooled. Most COTS technologies are not designed to operate in the types of environments faced by military and law enforcement units. It is important either to find systems capable of handling the weather environments or to modify systems carefully to ensure they will continue to operate.

The third lesson learned was that the "capabilities" claimed by the manufacturer are often much different than the actual performance. Most systems are tested in a laboratory environment, which can be closely controlled. Often, performance in a laboratory environment is significantly better than in an actual scenario. For example, the Crossbow data claimed a communications range of 150 to 250 feet. These data are significantly further than any distance achieved during testing, even with the motes at three feet above ground level. Sometimes the manufacturer's claimed performance is

less than what can be achieved. For example, Crossbow claims a detection range of 70 to 80 feet for large trucks. During the maximum detection range experiments, large trucks were routinely detected at ranges over 100 feet. Additionally, Crossbow claims the motes typically last ten hours on two AA batteries. The battery life tests showed that the actual lifetime is significantly longer. Ultimately, it is vitally important to test all COTS systems thoroughly before deploying in a military or law enforcement scenario to understand the actual performance in real-world scenarios.

The fourth lesson learned is that integrating COTS technologies for military applications can be very difficult. The entire COASTS 2006 network consisted of commercially available technologies. As a result, integration issues often arose. For example, the Vlinx servers were not capable of using some of the encryption techniques that the 802.11 mesh backbone used. Subsequently, the plans for encryption were discarded. Additionally, integrating the Crossbow serial data onto the 802.11 network proved to be more difficult than expected. Also, the manufacturer's support significantly impacts the success of integrating the technology. For example, the Vlinx technical support staff was excellent, often delivering solutions or assistance with little notice. The Crossbow technical support was not as helpful. While trying to integrate the Crossbow data into the C3Trak Shared Situational Awareness program, several problems arose. Crossbow was not helpful in trouble shooting or providing assistance to integrate its product into the application. Ultimately, the Crossbow sensors were not integrated into the application for demonstrations. If more time or better technical support been provided, the sensors might have been fully integrated. However, these difficulties helped to highlight the importance of cooperation between the user and manufacturer for applying the COTS technology to a unique and demanding situation.

C. FINAL EVALUATION

The prototyped sensor-camera network performed satisfactorily during the COASTS scenario demonstration in May, 2005. The sensing capabilities proved to be significantly better than expected. However, one must objectively evaluate the network based upon the metrics, MoP, and MoE discussed in previous chapters.

The sensor subsystem of the prototyped network performed satisfactorily during the evaluation experiments. The passive infrared sensor successfully detected humans and vehicles at ranges exceeding the MoE and MoP. The sensing capabilities were worth 40 percent of the sensor network's evaluation. The passive infrared was worth 24 percent of the total evaluation, with eight percent given to the ability to detect each of the categories of objects. Since the passive infrared sensor exceeded all of the minimum detection distance, full values were awarded. The magnetic sensor was worth 16 percent of the total evaluation. Again, the magnetic sensor detection ranges exceeded minimum values, so full values were awarded. The deployability of the sensor network was worth another 40 percent of the evaluation. The deployability in various operating environments absorbed 16 percent of the evaluation. The sensor network performed well in urban, wooded, and open terrains. The sensor network interoperability suffered in high-temperature environments due to problems with the Vlinx serial server. As a result, the network was awarded 14 of 16 points. The logistics aspect of the network was worth 24 percent of the evaluation. The network lost eight points due to the short battery life and was awarded 16 of the 24 points. A total of 10 of 14 points were awarded for interoperability due to the lack of native 802.11 networking capabilities. Finally, the network was awarded all six points for availability. When compared to the MoE, the sensor network was awarded a total of 86 out of 100 points. The sensor network satisfied nearly the entire MoP. Tables 17 and 18 depict the comparison with MoE and MoP values.

MoE			
Characteristic	**Points Allowed**	**Satisfied**	**Points Given**
PIR Human Detection	8	Yes	8
PIR Small Vehicle Detection	8	Yes	8
PIR Large Vehicle Detection	8	Yes	8
Magnetometer Small Vehicle Detection	8	Yes	8
Magnetometer Large Vehicle Detection	8	Yes	8
Urban, Wooded, Open Terrain	8	Yes	8
Adverse Climactic Conditions	8	No	6
Small Logistics Footprint	8	Yes	8
3+ Month Battery Life	8	No	0
Rapidly Deployable	8	Yes	8
Graphical Interface	2	Yes	2
Minimal Training	2	Yes	8
Native 802.11 Networking	10	No	0
COTS Technology	6	Yes	6
TOTAL	**100**		**86**

Table 17. Sensor MoE Final Analysis

MoP		
Characteristic	**Need/Want**	**Satisfied**
Less than 10 False Detections per Hour	Want	No
99 % Probability of Detection for Humans at 15 Feet	Need	Yes
99.5 % Probability of Detection for Vehicles at 15 Feet	Need	Yes
Ability to Classify and Object Based on Sensor Values	Want	Yes
Maximum Detection Range > 30 Feet for Humans	Need	Yes
Maximum Detection Range > 75 Feet for Vehicles	Need	Yes
Maximum Communications Range >= 120 Feet	Want	Yes at 1 Foot Elevation
Maximum Reassociation Range >= 60 Feet	Want	Yes at 1 Foot Elevation
Deployable in 10 minutes	Want	Yes
Operate with 802.11 b/g	Need	Not Native Capability, Yes with Additional Equipment
Multiple Sensor Types	Need	Yes
Battery Life > 3 Months	Need	No
Operate in Urban, Wooded, and Open Terrains	Need	Yes
Small Form Factor (Size)	Need	Yes

Table 18. Sensor MoP Final Analysis

The camera subsystem also performed satisfactorily during the testing and evaluation processes. The cameras' role in the network was to provide real-time visual information to the watch-stander. The MoE and MoP focused primarily on deployability, functionality, and interoperability. Deployability points were spread equally between logistic footprints, climactic limitations and power consumption, for a total of 25 percent of the evaluation. The Axis 213 was awarded 23 of the 25 points due to the problems associated with overheating. The ability to pan, tilt, and zoom the camera was worth another 25 percent of the evaluation. The Axis 213 received all 25 points due to the excellent capabilities and large field of view. The ability to choose between multicast and broadcast transmission was worth another 25 percent of the evaluation. When loaded

with the correct firmware version, the Axis 213 has the ability to perform in multicast or broadcast mode. As a result, the full 25 points were awarded. The ease of configuration was worth 12.5 percent of the evaluation. The camera has an intuitive and easy to use interface that allows specified users to change configurations remotely. The Axis 213 received the maximum award for configurability. Finally, 12.5 points were awarded for availability. The only negative evaluation for the Axis 213 camera is the troubles encountered due to heat. However, with slight modifications the camera performed well above expectations even in high-temperature environments. Tables 19 and 20 depict the comparison with the selected MoE and MoP.

MoE			
Characteristic	**Points Allowed**	**Satisfied**	**Points Given**
Multicast/Broadcast Optional	25	Yes	25
Controllable	25	Yes	25
Deployability	25	Yes	23
Easy to Configure	12.5	Yes	12.5
Immediately Available for Purchase	12.5	Yes	12.5
TOTAL	100		98

Table 19. Camera MoE Final Analysis

MoP		
Characteristic	**Need/Want**	**Satisfied**
MPEG Format	Want	Yes
Multicast Capability	Need	Yes
Control Pan/Tilt/Zoom	Need	Yes
IR Illumination	Need	Yes
20 Frames per Second	Need	Yes
Wireless Connectivity	Need	Not Natively, Requires Additional Equipment

Table 20. Camera MoP Final Analysis

As a whole, the prototyped network performed satisfactorily during the COASTS demonstrations in Thailand. Despite the successful performance in the scenarios, the prototyped network is not suitable for military applications but is well suited for law enforcement applications. Although the sensing capabilities of the Crossbow MSP410

Mote Security System far exceeded the minimum capabilities, several key negative aspects arose. The first, and most prominent, was the battery life of the system. Military operations require much longer battery lives than provided by the prototyped network. Law enforcement operations are typically much shorter and, therefore, require shorter on-station times. The second reason the system is appropriate for law enforcement applications and not military applications is significant performance degradation in extreme weather. Military forces routinely operate in harsh environments where any performance degradation is not acceptable. Components must not fail in high temperature. Beyond that, the significant reduction in communications ranges during rain storms would render the network useless. Although law enforcement units operate under adverse conditions, they tend to be less extreme than military operations. A third reason is the lack of native networking capabilities. The MSP410 base station is only designed to pass information using a serial connection. Connecting the serial base station to any existing network is difficult. Although 802.11 wireless networks might not be the best choice for tactical military networking, the system completely lacked the ability to transmit data along any other type of communications medium. Military operations require the system be able to integrate easily into a variety of tactical networks. However, 802.11 wireless networks are more suitable for law enforcement applications. The addition of the Vlinx Serial Server and the Mesh Dynamics access point do not provide a significant disadvantage for law enforcement. Further refinement of network components might make the network suitable for military applications, but as designed the prototyped network is not suitable for military operations.

D. AVENUES FOR FUTURE RESEARCH

This thesis provided an in-depth study of the prototyped network, yet several areas that are suitable for future research emerged. The avenues for future research can be divided into the broad categories of sensors, cameras, communications, integration, and power.

The sensor component of the network presents several areas for future research. The first area of research is to repeat the experiments with similar sensors from a different manufacturer. Other manufactures might use different components that have

better capabilities or battery lives. A comparison of two different sensor sets with the same types can be useful. Also, a variety of other sensor types are available. Several manufacturers currently make seismic sensors that can detect the small vibrations created by personnel and vehicles. A trade-off analysis between various sensor types will be useful in designing networks to meet the demands of military and law enforcement applications. Furthermore, physical security measures must be addressed for sensor networks. The network designed in this thesis had no physical security. Knowing if a sensor is moved or disabled by enemy forces is important. For example, GPS sensors could be used to detect if the sensor is relocated or adding biometric activation switches to prevent the sensors from being tampered with by enemy forces.

The camera network is an additional area for future research. This thesis used the Axis 213 camera, but several other camera models exist that might be better for such an application. For example, a wireless IP camera would be well suited for the application and would eliminate the need to connect the camera directly to an access point. Adding a night-vision camera is recommended for boarder protection applications, as most illegal immigration happens during low light hours. Finally, further research for camera cooling methods is necessary to deploy an integrated sensor-camera network in extreme environments such as Iraq.

A third area for future research concerns communications. This thesis attempted to determine the maximum communications distance for the network. Since many sensor networks use 802.15.4 or ZigBee protocols, it would be beneficial to understand how the low-power, low-data rate requirements affect RF propagation. In addition, communications security techniques can be researched. The Crossbow MSP410 motes use a frequency that is easily jammed and the low transmission power causes the frequency to be overpowered easily. Anti-jamming and encryption techniques can be useful for sensor networks used in military and law enforcement scenarios. Security remains a challenge for all wireless networks and is especially challenging given the low computing power of wireless sensor networks.

A fourth area that has many research applications is the integration of sensor-camera networks with emerging and existing capabilities. For example, most current

WSNs have custom user interface and do not interoperate easily with existing systems, such as Blue Force Tracker or other situational awareness programs. Crossbow, for example, uses the Mote-View program. Attempts to integrate the data into the C3Trak program proved difficult at best. A common data structure or extensible markup language can be created to allow programs to interact with a wide range of sensor networks easily. Sensor-camera networks can also be used to trigger automatic responses, such as launching unmanned vehicles, weapons aiming, and force protection actions. Lastly, the creation of "intelligent" weapons that activate only when enemy forces are present is possible. For example, "smart" landmines could only activate when enemy vehicles traverse the area.

The final area, and perhaps most important, is power management. Sensor-camera networks must be able to operate for several months without any direct human interaction. Creating more efficient components will help extend the on-station time of sensor-camera networks and increase the feasibility for military uses. Research can be done to create more efficient transmission protocols. Additionally, power engineers might develop better batteries or power sources. Alternative power sources such as solar cells can be designed to create a nearly limitless lifetime. Power management research will help achieve the goal of dense, long-life unattended sensor networks for real-time intelligence, surveillance, and reconnaissance.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. COASTS 2006 CONOPS

Coalition Operating Area Surveillance and Targeting System (COASTS) Thailand Field Experiment (May 2006) Concept of Operations

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ACRONYMS

AAR	After Action Report
ASR	Automated Speech Recognition
AUV	Autonomous (Unmanned) Underwater Vehicle
AT/FP	Anti-Terrorism/Force Protection
ATCD	Advanced Technology Concept Demonstration
BCA	Breadcrumb Administration
BKK	Bangkok
C2	Command & Control
C4ISR	Command, Control, Computers, Communications, Intelligence, Surveillance, and Reconnaissance
CIE	Common Information Environment
CMA	Cooperative Maritime Agreement
COASTS	Coalition Operating Area Surveillance and Targeting System
COC	Combat Operations Center
CONOPS	Concept of Operations
COTS	Commercial-Off-The-Shelf
DC	Direct Current
DEA	Drug Enforcement Agency
DoD	Department of Defense
DRDO	Defence Research Development Organization
DSSS	Distributed Sequence Spread Spectrum
FCC	Federal Communications Commission
FLAK	Fly-away Kit
FLTSATCOM	Fleet Satellite Communications
GHz	Gigahertz
GPS	Global Positioning System
GUI	Graphical User Interface
HA/DR	Humanitarian Assistance/Disaster Relief
IEEE	Institute of Electrical and Electronic Engineers
IIFC	Interagency Intelligence Fusion Center
ISR	Intelligence, Surveillance, and Reconnaissance

JI	Jemaah Islamiyah
JIATF-W	Joint Interagency Task Force West
JUSMAGTHAI	Joint US Military Advisory Group Thailand
KIAS	Knot Indicated Air Speed
Li-Ion	Lithium Ion
LIO	Leadership Interdiction Operation
LCS	Littoral Combat Ship
LM	Language Model
MALSINDO	Malaysia Singapore Indonesia
Mbps	Mega bits per second
MCP	Mobile Command Post
MDA	Maritime Domain Awareness
MDP-RG	Maritime Domain Protection Research Group
MDS	Mercury Data Systems
MIO	Maritime Interdiction Operation
MOE	Measures of Effectiveness
MOP	Measures of Performance
MOSP	Multi-Mission Optronic Stabilized Payload
NPS	Naval Postgraduate School
NSW	Naval Special Warfare
OFDM	Orthogonal Frequency Division Multiplexing
OSD	Office of the Secretary of Defense
OTH	Over the Horizon
OTHT	Over the Horizon Targeting
PDA	Personal Data Assistant
PSYOP	Psychological Operations
RF	Radio Frequency
RHIB	Rigid Hull Inflatable Boat
ROE	Rules of Engagement
RTA	Royal Thai Army
RTAF	Royal Thai Air Force
RTARF	Royal Thai Armed Forces
RTN	Royal Thai Navy

SATCOM	Satellite Communications
SBU	Special Boat Units
SOF	Special Operations Forces
SOP	Standard Operating Procedure
SSA	Shared Situational Awareness
SSA	Shan State Army
SURA	Shan United Revolutionary Army
TNT FE	Tactical Network Topology Field Experiment
TTS	Text to Speech
UAV	Unmanned Aerial Vehicle
USA	United States Army
USAF	United States Air Force
USCG	United States Coast Guard
USG	United States Government
USMC	United States Marine Corps
USN	United States Navy
USPACOM	United States Pacific Command
USSOCOM	United States Special Operations Command
UWSA	United Wa State Army
UNODC	United Nations Office on Drugs & Crime
VBSS	Visit, Board, Search, & Seizure
VA	Voice Authentication
VOIP	Voice over Internet Protocol
VLV	Variable Length Verification
VM	Verification Model
VUI	Voice User Interface
VV	Voice Verification
Wi-Fi	Wireless Fidelity
Wi-Max	Wireless
WLAN	Wireless Local Area Network

LIST OF EFFECTIVE CHANGES

Date	Revision Number	Description	Point of Contact
31OCT05	1	Document submitted to COASTS Program Manager for review	Jim Ehlert
19NOV05	2	Document submitted to COASTS Program Manager for review	Jim Ehlert
01DEC05	3	Document submitted to COASTS Program Manager for review	Jim Ehlert
22DEC05	4	Document submitted to COASTS Program Manager for review	Jim Ehlert
30DEC05	5	Document submitted to COASTS Program Manager for review	Jim Ehlert

1.0 PURPOSE.

This document describes the FY2006 Concept of Operations (CONOPS) for the development and implementation of the Naval Postgraduate School (NPS) research program entitled the Coalition Operating Area Surveillance and Targeting System (COASTS). The COASTS field experimentation program supports U.S. Pacific Command (USPACOM), Joint Interagency Task Force West (JIATF-W), Joint U.S. Military Advisory Group Thailand (JUSMAGTHAI), U.S. Special Operations Command (USSOCOM), NPS, Royal Thai Armed Forces (RTARF), and the Thai Department of Research & Development Office (DRDO) science and technology research requirements relating to theater and national security, counter-drug and law enforcement missions, and the War On Terror (WOT). This CONOPS is primarily intended for use by the NPS and RTARF management teams as well as by participating commercial partners. However, it may be provided to other U.S. Government (USG) organizations as applicable. This document describes research and development aspects of the COASTS program and establishes a proposed timetable for a cap-stone demonstration during May 2006 in Thailand.

LIMITED DISTRIBUTION: Distribution limited to the Department of Defense (DoD), U.S. DoD contractors, and to U.S. Government Agencies supporting DoD functions, and is made under the authority of the Director, DMA. Foreign governments, contractors, and military personnel contributing to the COASTS research project are included within the limited distribution per the purview of the COASTS Program Manager.

1.1 BACKGROUND.

The COASTS programmatic concept is modeled after a very successful ongoing NPS-driven field experimentation program entitled the NPS-U.S. Special Operations Command Field Experimentation Program (NPSSOCFEP). NPSSOCFEP is executed by NPS, in cooperation with USSOCOM and several contractors, and has been active since FY2002. Program inception supported USSOCOM requirements for integrating emerging wireless local area network (WLAN) technologies with surveillance and targeting hardware/software systems to augment Special Operations Forces (SOF) missions. NPSSOCFEP has grown significantly since inauguration to include 10-12 private sector companies who continue to demonstrate their hardware/software capabilities, several DoD organizations (led by NPS) who provide operational and tactical surveillance and targeting requirements, as well as other academic institutions and universities who contribute a variety of resources.

1.1.1 NPSSOCFEP Specifics.

NPSSOCFEP conducts quarterly 1-2 week long complex experiments comprising 8-10 NPS faculty members, 20-30 NPS students, and representatives from multiple private companies, DoD and US government agencies. Major objectives are as follows:

- Provide an opportunity for NPS students and faculty to experiment/evaluate with the latest technologies which have potential near-term application to the warfighter.
- Leverage operational experience of NPS students and faculty
- Provide military, national laboratories, contractors, and civilian universities an opportunity to test and evaluate new technologies in operational environments
- Utilize small, focused field experiments with well-defined measures of performance for both the technologies and the operator using the technologies
- Implement self-forming / self-healing, multi-path, ad-hoc network w/sensor cell, ground, air, and satellite communications (SATCOM) network components

1.1.2 NPSSOCFEP Limitations.

1.1.2.1 Sensitivities with Foreign Observers/Participants.

Certain hardware, software, and tactics/techniques/procedures (TTP's) implemented at NPSSOCFEP are classified or operationally sensitive, and as a result sponsors have not agreed to foreign military partnerships. However, DoD requirements exist for U.S. military forces to operate in coalition environments (which serve to strengthen relationships with foreign military partners) and to execute missions globally. Since NPSSOCFEP remains primarily a US-only event, COASTS was designed to address coalition inter-operability exchange and cooperative R&D.

1.1.2.2 Meteorological, Hydrographic, & Geographic Considerations.

The majority of wireless network topology research conducted by the NPS has occurred in the California Central Coast area where vegetation and climate is not representative of the Pacific Area of Responsibility (AOR)—a likely deployment location for tactical or operational WLAN and surveillance/targeting technologies. Higher temperatures and humidity, as well as denser vegetation in regions like Southeast Asia will likely create WLAN and sensor performance problems. This was proven in data collected during the COASTS 2005 deployment, and will be further examined in the 2006 deployment.

1.1.3 COASTS 2005.

1.1.3.1 Purpose.

COASTS 2005 leveraged and integrated the technological expertise of NPS's education and research resources with the science and technology and operational requirements of the RTARF. This was done using WLAN technologies (see Figure 1 next page) to fuse and display information from air and ground sensors to a real-time, tactical, coalition enabled command and control (C2) center. The additional benefit of this first COASTS field experiment was to demonstrate USPACOM commitment to foster stronger multi-lateral relations in the area of technology development and coalition warfare with key Pacific AOR allies in the WOT - results from the May 2005 demonstration were provided to representatives from Thailand, Singapore, Australia, South Korea and the U.S.

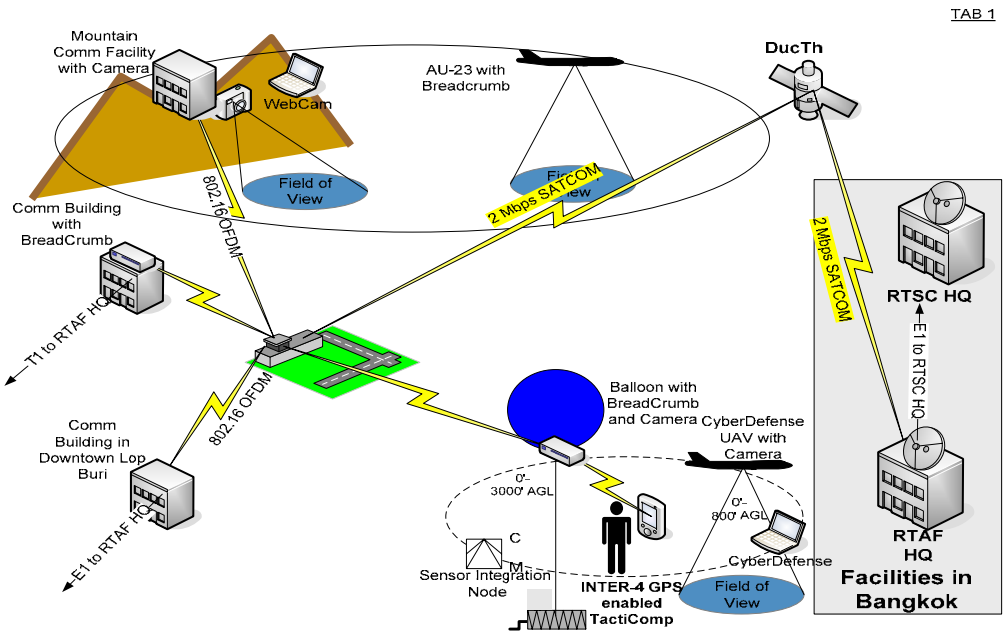


Figure 1. COASTS 2005 Network Topology

1.1.4. COASTS 2006.

1.1.4.1 Purpose.

COASTS 2006 will expand upon the original field experiment conducted during last year's deployment to Wing 2, Lop Buri, Thailand. This year's network topology (see Figures 2 and 3 on following pages) will advance research relative to low-cost, commercially available solutions while integrating each technology/capability into a larger system of systems in support of tactical action scenarios. The demonstration planned for May 2006 is an air, ground, and water-based scenario (details provided below), occurring just north of Chiang Mai, Thailand. The scenario encompasses first-responder, law enforcement, counter-terrorism, and counter-drug objectives. The tactical information being collected from the scenario will be fused, displayed, and distributed in real-time to local (Chiang Mai), theater (Bangkok), and global (Alameda, California) C2 centers. This fusion of information leads to the validation of using wireless communication mediums to support redundant links of the National Information Infrastructure, as well as to test and evaluate the 'last mile' solution for the disadvantaged user. Continuing with last year's research theme, COASTS 2006 will again: (1) examine the feasibility of rapidly-deploying networks, called "Fly-away Kits" (FLAK) and (2) explore sustainment considerations with respect to a hostile climatic (temperature, humidity, wind, etc.) environment. Network improvements will include the testing and evaluation of new 802.11 mesh LAN equipment, the refinement of a jointly-developed (NPS and Mercury Data Systems) 3-D topographic shared situational awareness (SSA) application called C3Trak, the integration of "satellite in a suitcase" (portable satellite communication equipment) technology, enhanced unattended ground and water-based sensors, new balloon and UAV designs, portable biometric devices, portable explosive

residue detecting devices, and revised operational procedures for deployment of the network. Further explanation of the network technology can be found in Appendix A.

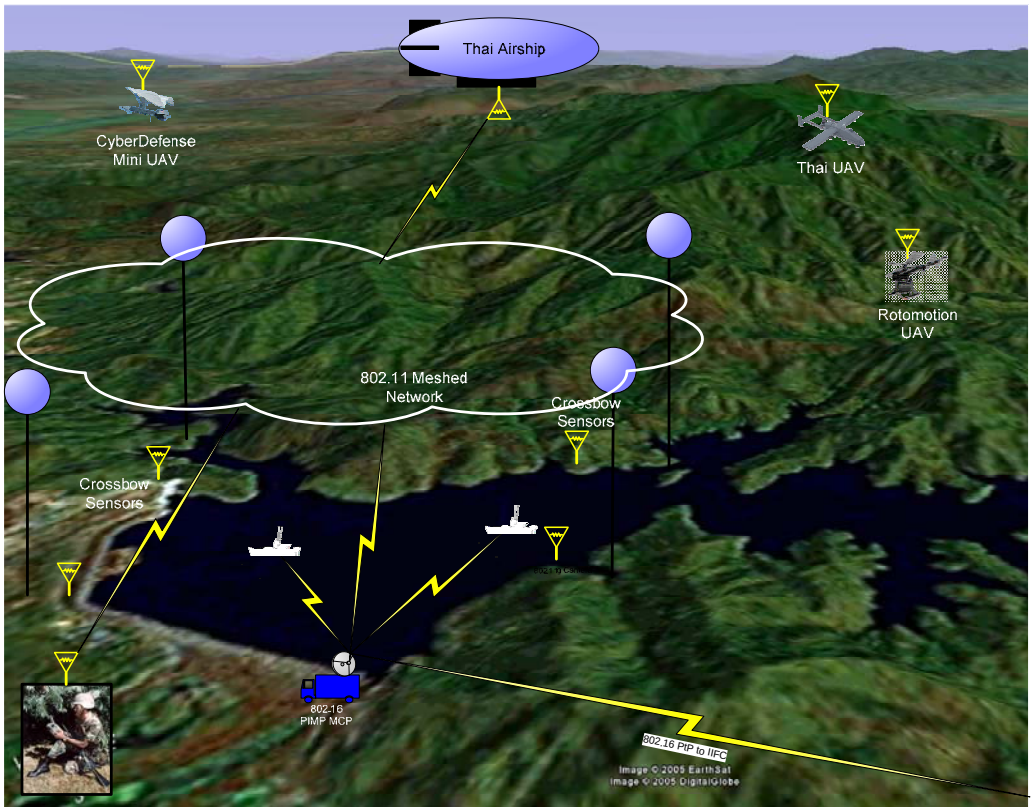


Figure 2. COASTS 2006 Topology: Mae Ngat Dam

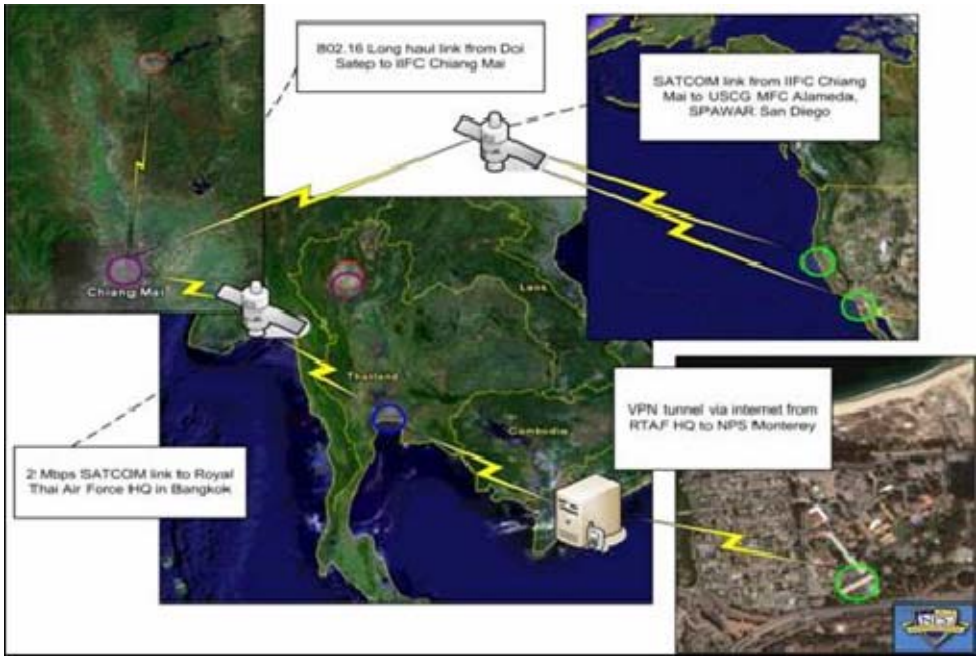


Figure 3. COASTS 2006 Global Network Topology

1.2 REFERENCES.

- Joint Publication (JP) 3-13, "Joint Doctrine for Information Operations", 9 October 1998
- JP 3-03, "Joint Doctrine for Interdiction Operations", 10 April 1997
- JP 3-54, "Joint Doctrine for Operations Security", 24 January 1997
- JP 6-0, "Joint Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations", 30 May 1995
- JP 3-06, "Joint Doctrine for Riverine operations", 11 Sep 1991
- Joint Vision 2010
- Joint Vision 2020
- Network-Centric Warfare: DoD report to Congress, 21 July 2001
- DoD 2000.12-P, "Antiterrorism Strategic Plan", 15 June 2004
- DoD 2000.12, "US Navy Instruction Antiterrorism/Force Protection(AT/FP)", 13April 1999
- COASTS Concept of Operations 2005
- COASTS OPORD, March 2005
- COASTS OPORD, April 2005
- National Strategy for Combating Terrorism, February 2003
- National Security Strategy, September 2002
- National Strategy for Maritime Security, September 2005
- Challenge for a New Era: Chief of Naval Operations Guidance for 2006, September 2005
- COMSECONDLFT message (DTG 041359Z OCT 05)
- United Nations Office of Drugs & Crime (UNODC) "Strengthening Law Enforcement in Eastern Asia" 26 November 2005
- United Nations Office of Drugs & Crime (UNODC) World Drug Report 2005

1.3 SCOPE.

This concept of operations (CONOPS) applies to all aspects of the COASTS project from date of issue through the May 2006 Thailand-based demonstration. This document is intended to provide critical information regarding the planning and execution of all aspects of the FY2006 field experimentation program. Additionally, this CONOPS provides a technical and tactical framework for complex system demonstrations used in coalition environments. This document will cover the use of COASTS as a stand-alone or networked capability focused on security mission profiles that can be enhanced by the employment of COASTS technologies.

2.0 OVERVIEW.

2.1 CURRENT SITUATION.

2.1.1 U.S. Perspective.

The risk of asymmetric threats to U.S. national security has outpaced the danger of traditional combat operations against a first-tier opposing military force. National security requirements are increasingly focused on facing non-military, non-traditional, asymmetric threats: piracy, terrorism, narcotics smuggling, human trafficking, weapons of mass destruction, and other transnational threats. Furthermore, with the always accelerating movement of globalization stretching U.S. interests further away from domestic borders, the national security issues of allies and other friendly nations are as vital to the U.S. as American domestic security issues.

Last year in Sacramento, California over 73,000 "Yaa Baa" (crazy medicine) methamphetamine pills were confiscated by law enforcement. Yaa baa is produced primarily by the United WA State Army (UWSA), an ethnic insurgency force operating within the Burmese portion of the Golden Triangle region of Southeast Asia. These drugs were cultivated in the Golden Triangle, passed across the borders of multiple nations in Southeast Asia, and across the Pacific Ocean through various other international harbors such as Hong Kong or Singapore, as well as at least one domestic U.S. harbor. As easily as these drugs move into the interior of America, so could any multitude of other national security threats such as chemical and biological weapons of mass destruction.

Numerous law enforcement, corporate and bi-lateral, multilateral, and international governmental initiatives are attempting to address these security issues on a variety of levels. JIATF-W is constructing data/intelligence fusion centers like the Inter-agency Intelligence Fusion Center (IIFC) in Chiang Mai, Thailand to enable joint and coalition intelligence collection for combined multi-national operations. The Regional Maritime Security Initiative (RMSI) and Cooperative Maritime Agreement (CMA) Advanced Technology Concept Demonstration (ATCD), focus on transnational open ocean counter-piracy and counter-terrorism, and investigate the formulation of more intelligence fusion centers and multilateral coastal patrolling agreements, i.e. MALSINDO respective to the Straits of Malacca.

The importance of a coalition-oriented focus for modern Maritime Domain Awareness and Protection operations is not lost on U.S. combatant commanders. In a recent naval message, all numbered fleet commanders stated their number one Command, Control, Computers, Communications, Intelligence, Surveillance, and Reconnaissance (C4ISR) requirement is improved coalition communications. Current and future operational capabilities are tightly tied to improved interoperability with U.S. allies in the operational theater. As reflected by the increasing number of requests to NPS from foreign partners, there is an immediate requirement for low-cost, state-of-the-art, real-time threat warning and tactical communication equipment that is also rapidly scaleable

based on operational considerations. This issue has become especially apparent in the face of the overwhelming mission requirements placed on US forces conducting the WOT.

The WOT extends globally where nations are engaged in direct action against numerous forces employing asymmetric tactics. In Thailand, the separatist insurgency in the southern provinces is connected to various transnational terrorist organizations which have struck against both the U.S. and its allies, to include both the Jemaah Islamiyah (JI) and Al-Qaeda.

Further exacerbating the above situation, most current tactical systems lack the capability to rapidly enable a common information environment (CIE) amongst air, surface, and sub-surface entities via a self-forming, self-authenticating, autonomous network. Although commercial-off-the-shelf (COTS) technologies exist that can satisfy some of these requirements, these same technologies typically do not meet all of the DoD and coalition partner requirements associated with WOT and other security missions. Hence a central role of the COASTS field experimentation program is to demonstrate that NPS, in conjunction with coalition partner R&D organizations, can integrate COTS capabilities into a larger system of systems to potentially satisfy technical and tactical mission requirements.

2.1.2 Thailand Perspective.

The Golden Triangle Region of Southeast Asia, which includes the border regions of Thailand, Laos, Myanmar, and China, cultivates, produces, and ships enough opium and heroin to be second only to Afghanistan as a global production region. Furthermore, the Western portion of the Golden Triangle, located along most of the Burmese border with Thailand, is the largest yaa baa methamphetamine producing region in the world. Over one million addicts of yaa baa currently reside in Thailand.

2.1.2.1 Burma

Burma remains the world's second largest producer of illicit opium with an estimated production of 292 metric tons in 2004. It is estimated that less than 1% of Burma's annual opium production is intercepted - the rest is smuggled out through China or Thailand onto the world market. Perhaps more significant, Burma and the Golden Triangle is the largest methamphetamine-producing region in the world. A 1999 survey of 32 of Thailand's 76 provinces showed that nearly 55 percent of youths in secondary and tertiary education were using methamphetamines. Not surprisingly, Thailand views the opium and methamphetamine production of the Golden Triangle as a threat to national security and is eager to stem the flow of these drugs across its national borders.

2.1.2.2 The United Wa State Army (UWSA).

The remote jungles that divide Burma and Thailand are controlled by the UWSA, a powerful militant organization comprised from the Wa ethnic group. They have a historic reputation as a savage people; in fact some tribes practiced headhunting as late as the 1970's. The Wa, serving as the primary fighting force of the Burmese Communist Party (BCP) until the BCP's disintegration in 1988, took over the BCP's drug operations and expanded upon them. The UWSA is, a well-equipped military force of approximately 20,000 soldiers, and is the largest drug-producing and trafficking group in Southeast Asia, producing heroin, methamphetamine, and possibly Methylenedioxy Methamphetamine (MDMA), or "Ecstasy".. The UWSA buys opium from the Kokang Chinese, the Shan United Revolutionary Army (SURA), and others to use in their increasing number of refineries – currently estimated at more than 50. The Southern Military Region of the UWSA is located in the Mong Yawn Valley near the Burma–Thailand border. Involved in the drug trade for decades, the Wa has increasingly switched to the production of methamphetamine pills due to international pressure to cut opium production. Due to increasing friction between the UWSA and the Burmese government - because of law enforcement efforts and greater power sought by regional Communists - there has been a significant increase of violence and traffic across the Thai border. As a result, a coalition effort consisting of Thai and U.S. forces was created in the Burma-Thailand border area of the Golden Triangle.

2.1.2.3. Shan United Revolutionary Army (SURA).

Competing with the Wa in the drug smuggling activity is the Shan ethnic group in cooperation with the Shan United Revolutionary Army (SURA). The SURA contains approximately 1,500 ethnic Shan soldiers and is one of the few remaining ethnic insurgent groups that have not agreed to a cease-fire arrangement with the Burmese Government. Recent reporting indicates that the SURA is collecting taxes from Shan traffickers and is forcing farmers to grow opium. Due to hostilities with the Wa in Burma, over 200,000 Shan refugees have crossed into Thailand since 2000 where most end up as illegal laborers.

2.1.3 U.S. and Thai Partnership.

It is the intent of the COASTS field experimentation program to demonstrate TTPs that: (1) potentially reduce or mitigate drug trafficking across the Thai-Burma border, (2) provide actionable information (real-time) to local, regional, and strategic level decision-makers, and (3) shorten the sensor-to-shooter cycle.

2.2 SYSTEM SUMMARY.

COASTS is an individual and small unit network-capable communication and threat warning system using an open, plug-and-play architecture, which is user-configurable, employing air balloons, wireless ad-hoc networks, UAVs, SSA software

applications, biometrics capabilities, portable and fixed ground and water based integrated sensors, and personnel equipped with Tacticomp/Antelope or similar PDAs, all communicating via wireless network technology.

2.3 CAPABILITIES.

COASTS 2006 provides a mobile field experiment bed environment for U.S. and Thailand in support of R&D, integration, operational testing, and field validation of several emerging wireless technologies and equipment suites. The following research elements will be addressed:

- 802.11 b Distributed Sequence Spread Spectrum (DSSS)
- 802.11a/g Orthogonal Frequency Division Multiplexing (OFDM)
- 802.16 OFDM (Stationary)
- 802.16 OFDM (Mobile)
- SATCOM
- Situational Awareness Overlay Software
- Wearable Computing Devices
- Air, Ground, and Water Integrated Sensors
- Mobile C2 Platforms
- Unmanned Aerial Vehicles (UAVs) (Fixed wing)
- UAVs (Rotary wing)
- Unmanned Multi-environment micro vehicles
- Ultra-wide Band Integrated Sensors
- Deny-GPS Inertial Gyro technology
- Network Security Applications
- Compression software applications
- Biometrics applications

2.4 MAJOR COMPONENTS.

While the final configuration of the COASTS 2006 system may evolve further, the following core elements represent the major system components:

- Supplied by Thailand:
  - Chiang Mai IIFC
  - Lighter-than-air Vehicle (LTAV)
  - L-39 Fighters (2)

- Royal Thai Air Force (RTAF) Unmanned Aerial Vehicles (UAV)
- Mobile Command Platform (MCP) – Figure 4
- Wing 41 facilities
- AU-23 configured with 802.11g connectivity
- Royal Thai Army (RTA) interdiction squad

Figure 4. Thai Mobile Command Platform

- Supplied by NPS:
  - Situational awareness common operating picture (SA COP) systems
  - Tethered balloons and associated hardware – Figure 5
  - Airborne camera system for balloon and/or UAVs – Figure 6
  - Wearable Computing Devices (INTER-4 Tacticomp) – Figure 7
  - Three (3) laptops for use in the NMC
  - Three (3) Modular PCs (Antelope)
  - 802.11a/b/g network devices – Figure 8
  - 802.16 OFDM network devices – Figure 9
  - Deny GPS

- Rotomotion UAV – Figure 10
- CyberDefense UAV – Figure 11
- Helia-Kite Network Extender – Figure 12
- Network Security Applications
- Small boat FLAKs
- Biometric devices – Figure 13
- Morphing Micro Air-Land Vehicle (MMALV) – Figure 14

Figure 5. Tethered Balloon

Figure 6. Airborne camera system for balloon and/or UAVs

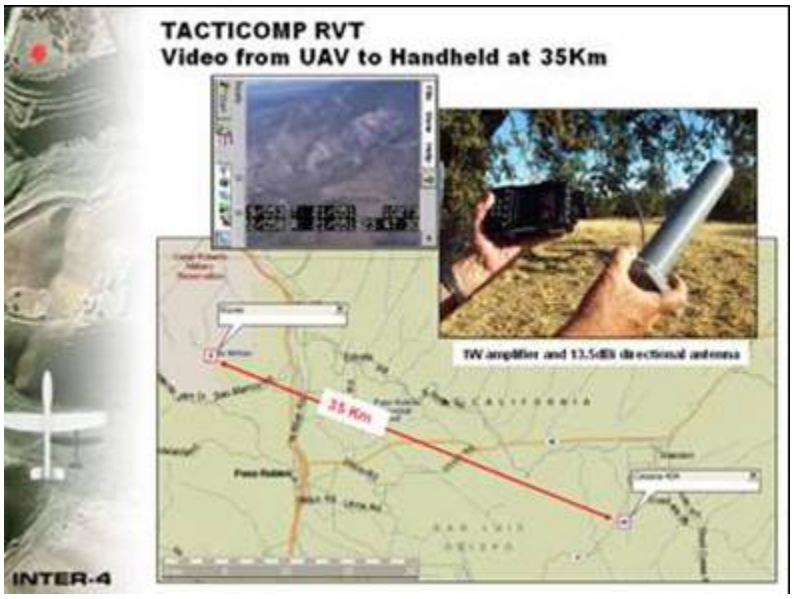


Figure 7. INTER-4 Tacticomp Handheld GPS Enabled Networked Situational Awareness Tools

Figure 8. 802.11a/b/g network Mesh Dynamics Unit

Figure 9. Red Line Communications 802.16 Suite

Figure 10. Rotomotion VTOL UAV

Figure 11. Cyber Defense UAV

Figure 12. Helia-Kite Network Extender

Figure 13. Biometric Collection Device

Figure 14. Morphing Micro Air-Land Vehicle (MMALV)

2.5 CONFIGURATIONS.

The May 2006 COASTS demonstration will have four basic configurations: (1) a command, control, collection, and communication suite; (2) a threat warning system; (3) an intelligence collection system; and (4) a Global Law Enforcement Interdiction database.

3.0 CONCEPT OF OPERATIONS.

3.1 USERS.

Generally, the COASTS 2006 participants will focus on creating an international interaction mechanism for U.S. military forces, to include NPS, to collaborate with Thailand research & development organizations and military forces to support WOT objectives and internal/external Thai security requirements.

The primary users during the May 2006 demonstration will be the military and civilian NPS students and faculty, JIATF-W personnel, JUSMAGTHAI personnel, and various units from the RTARF. Secondary users may include members of the Singapore Armed Forces (SAF), Malaysian Maritime Enforcement Agency (MMEA), Japanese Self Defense Force (JSDF), Republic of the Philippines Army, and the Australian Army. Tertiary users will be the various vendors providing equipment and technical expertise to include Cisco Systems Inc., Redline Communications, Mercury Data Systems, CyberDefense Systems, Roto-motion Inc, Identix, and INTER-4. Specific vendor contributions shall be discussed in the Appendix section of this document. The NPS, RTARF, and vendor team will integrate COASTS into a system to facilitate surveillance and monitoring of simulated "areas of interest".

3.2 COASTS SUPPORT FOR PRINCIPAL MISSION AREAS.

As per Joint Doctrine, COASTS will directly support organizing, training, and equipping U.S. military forces and the RTARF in nine principal mission areas:

Direct Action (DA): The primary function of COASTS during DA missions is to provide Force Protection. DA missions are typically short-duration, offensive, high-tempo operations that require real-time threat information presented with little or no operator interface. COASTS will augment other capabilities in direct support of DA from an over-watch position. COASTS in support of DA will target collection to support threat warnings relevant to that specific operation and provide automated reporting to the Tactical Operations Center (TOC) for potential threats relevant to a specific mission. COASTS may also be used as the primary source of threat information in the absence of other capabilities. Threat information presented by COASTS is intended to be relevant, real-time or near real-time, and within the area of operation.

Tactical Reconnaissance (TR): The primary purpose of a TR mission is to collect information. COASTS will augment other capabilities to obtain or verify information concerning the capabilities, intentions, locations, and activities of an actual or potential adversary. COASTS will support the full range of information and communication functions. COASTS will support operators with the rapid collection, processing, analysis, and dissemination of information. COASTS will analyze how performance in this mission is influenced by meteorological, hydrographic, and geographic considerations.

Foreign Internal Defense (FID): COASTS will assist Host Nation (HN) military and paramilitary forces, with the goal to enable these forces to maintain the HN's internal stability.

Combating Terrorism (CBT): COASTS will support CBT activities, to include anti-terrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), conducted to oppose terrorism throughout the entire threat spectrum.

Civil Affairs (CA): COASTS will assist CA activities in peacetime to preclude grievances from flaring into war and during hostilities to help ensure that civilians do not interfere with operations and that they are protected and cared for in the combat zone.

Counter-proliferation of Weapons of Mass Destruction (WMD): COASTS will assist traditional capabilities to seize, capture, destroy, render safe, or recover WMD. COASTS can provide information to assist U.S. military forces and coalition partners to operate against threats posed by WMD and their delivery systems.

Information Operations (IO): COASTS can augment actions taken to affect adversary information and information systems while defending one's own information and information systems. IO applies across all phases of an operation and the spectrum of military operations.

Counter-narcotic Operations: COASTS will augment JIATF-W, U.S. Embassy Bangkok, and Thai law enforcement efforts to reduce the level of transnational narcotic smuggling across international borders in Southeast Asia. Since the "Golden Triangle" region is the second largest producer of the world market's heroin and methamphetamines, this regional reduction will further contribute to worldwide counter-drug efforts.

Maritime Security: COASTS will utilize a C4ISR capability for small boats that can be used for connectivity between any small boat assets capable of conducting maritime terrorism interdiction operations. The modular usage of FLAK technology makes small boat interdictions ISR-mission capable. Junk Force, U.S. Coast Guard (USCG), United States Navy (USN), Small Boat Unit (SBU), Naval Special Warfare (NSW), Special Operations Force (SOF), etc. will all potentially benefit from the COASTS 2006 research field experiment.

Maritime Interdiction Operation/Leadership Interdiction Operation (MIO/LIO): Visit Board, Search, and Seizure (VBSS) operations are conducted by all U.S. and coalition forces, to include various law enforcement agencies. Various network topologies tested in COASTS will enhance the C4ISR capabilities of conducting these operations. Historically, these missions have been removed from the digital divide of wireless capabilities for operations, and will be a focus point in COASTS 2006.

Training: The demonstration will be conducted in coordination with the US military forces, Thailand law enforcement academies, and various Thai military communications divisions. The technical and doctrinal information-sharing will contribute to the coalition operational capability of the Thai and U.S. civilian-military forces.

Psychological Operations (PSYOP): As a vital IO tool in counter-insurgency and counter-terrorism operations, the COASTS network will analyze the ability of the COASTS network to be used for PSYOP missions in the tactical environment.

3.2.1 Thailand Requirements.

3.2.1.1 Thailand Requirement Overview.

Thailand has a 2100 kilometer border with Burma that requires its military assets to patrol, as well as to provide surveillance, monitoring and targeting to combat drug smugglers and human traffickers from entering the country via Burma. This illicit drug smuggling/human trafficking problem is significant for both Thailand and the U.S. as these activities may potentially support financing and operations of international terrorist organizations.

In addition, some of the illegal drugs that successfully evade Thailand's security infrastructure are ultimately taken to the U.S. via containerized shipping through the Straits of Malacca and Singapore Straits. The RTAF has been assigned the responsibility of aerial patrols of the Thailand/Burma border areas while the Royal Thai Army (RTA) 3rd Army maintains cognizance for ground–based security and surveillance.

Likewise, the recent difficulties in the southern regions of Thailand pose potential serious security concerns. In an attempt to de-escalate tensions RTARF assets, most specifically the RTA 4th Army, have been deployed to the region. Continued difficulty, or an escalation in unrest, might lead to instability along the border as well as impacting the stability postures of other nations within the region.

The insurgency in the Southern Provinces has greatly affected Thailand's national security. Consistent asymmetric attacks from insurgents have taken a significant toll on the Thailand military forces. Increasing both ground and maritime security through more capable ISR will enable Thailand to reduce asymmetric attacks against civilian and military targets.

Finally, Thailand has been engaged in efforts, primarily in the Gulf of Thailand and surrounding territorial waters, to mitigate small boat activity involved in the illegal distribution of weapons and ammunition.

3.2.1.2 COASTS Support to Thai Requirements.

The RTARF has previously approached NPS for collaboration using UAVs and related surveillance/targeting technologies to augment their land and maritime border patrolling resources. The RTARF is considering using UAV's and sensor meshes to help control their northern and southern borders.

3.3 COASTS IMPLEMENTATION AND OBJECTIVES – PHASED APPROACH.

The overall COASTS program uses a phased spiral development to implement the Thailand-based demonstration.

Phase I: This initial phase will consist of the integrated demonstration (Test I) at Point Sur, California from 5-9 December, 2005. The NPS COASTS team will use the Point Sur test as a reduced-scale baseline in support of the deployable COASTS network.

Phase II: Following the 2005-2006 holiday break, the COASTS Program Manager will attend a mid-planning conference with the Thai leadership in Bangkok and Chiang Mai, Thailand on January 23-27, 2006. In addition, the 802.16 Wi-max link between the Joint Operations Area (Mae Ngat Dam) and the IIFC will be constructed and tested. Based on the information and decisions derived from this conference, a second integrated test (Test II) will be conducted at Point Sur on February 6-10, 2006. Equipment, network, and scenario implementation decisions will be finalized at the conclusion of Test II. The final planning conference will be conducted on February 20-24, 2006 in Bangkok, Thailand.

Phase III: The third phase will commence with the complete COASTS system deployment from NPS to Thailand, and subsequent set-up and testing, occurring in late March 2006 (exact dates are TBD, but are expected to be March 20-31, 2006). The primary focus of this phase will be to identify and mitigate any shortfalls relating to administration, deployment, and operation of the COASTS network. Upon completion of successful testing and operation, the COASTS network will be disassembled and stored at JUSMAGTHAI and/or Wing 41.

Phase IV: This fourth and final phase will consist of the actual operational demonstration, occurring May 22-31 2006. Since the timing of the COASTS demonstration is in parallel with the COBRA GOLD 2006 Command Post Exercise (CPX), COBRA GOLD and senior RTARF leadership will be available to receive the COASTS executive summary and observe the actual system demonstration.

3.3.1 Phase I - Work Up.

Phase I consists of the following.

Milestones Completed:

- Conducted a July 2005 After Action Report (AAR) debrief for U.S. and Thai COASTS 2005 participants, to include full disclosure on all pertinent issues concerning the deployment and demonstration testing.
- Conducted an August 2005 site survey that included Wing 41, the Mae Ngat Dam Joint Operations Area (JOA), and the IIFC. Baseline signal readings were taken at the Mae Ngat Dam as well as GPS positions for future network asset placements.

- Completed an October 2005 concept development conference at the NPS with RTARF officers.

Major Issues Remaining:

- Operational and Technical details of the LTAV?
- Cross-channel interference from the RTAF 802.11g capability?
- Availability of the MCP?
- Power at the Mae Ngat Dam?
- Lack of thesis students for key operational/technical areas?
- GPS positions of cell-phone towers in Chang Mai, Thailand?
- Baseline tests during the Pt Sur Integrated tests?
- Secondary tests during the second Pt Sur Integrated tests?
- Mini-test schedules and locations
- MIFC VPN planning meeting
- Biometric planning meeting
- NSG Monterey training & operational schedule

3.3.2 Phase II – Pt Sur Integrated Test I & II

Phase II entails the collection of individual nodal and integrated tests required to prepare for the COASTS deployment to Thailand in March and May 2006. On December 3-9, 2005, COASTS members conducted the first integrated test of equipment at PT Sur California. These tests included:

- Initial Network Construction
- 802.11 antenna configuration, range, and power testing
- Deny GPS testing
- Baseline Data Collection
- Initial Logistics management
- Mobile and Stationary 802.16 OFDM testing

Overall, the completed tests identified further research avenues, equipment requirements, and logistics needs the team must assess prior to the deployment to Thailand in March 2006.

Over the Holiday break, individual node leaders will conduct tests to finalize their baseline testing parameters prior to the second and third integrated tests. These mini-tests will focus on antenna configuration, power management, and the removal of extraneous material prior to deployment. The first integrated tests to follow these will be conducted

at the former Fort Ord North of the Naval Postgraduate School in Monterey, CA. The next integrated test will be of the final deployable network in February 2006.

3.3.3 Phase III – Movement to Site

Phase III continues the planning and preparation for the May 2006 demonstration to include movement of personnel and equipment to on-site Thailand locations designated for the demonstration. Further, on site testing will be accomplished during Phase III prior to beginning Phase IV preparations. The March 2006 deployment, tentatively scheduled for 20-24 March 2006, will include transportation, network set-up, and initial baseline testing for the full demonstration.

3.3.4 Phase IV – May 2006 Demonstration.

The actual COASTS project demonstration will attempt to prove a low-cost, state of the art, rapidly deployable, scalable tactical system to monitor a land/sea border region using unattended air and ground sensors connected through an assortment of wireless network technologies (refer to Figure 15). Specific details are provided below:

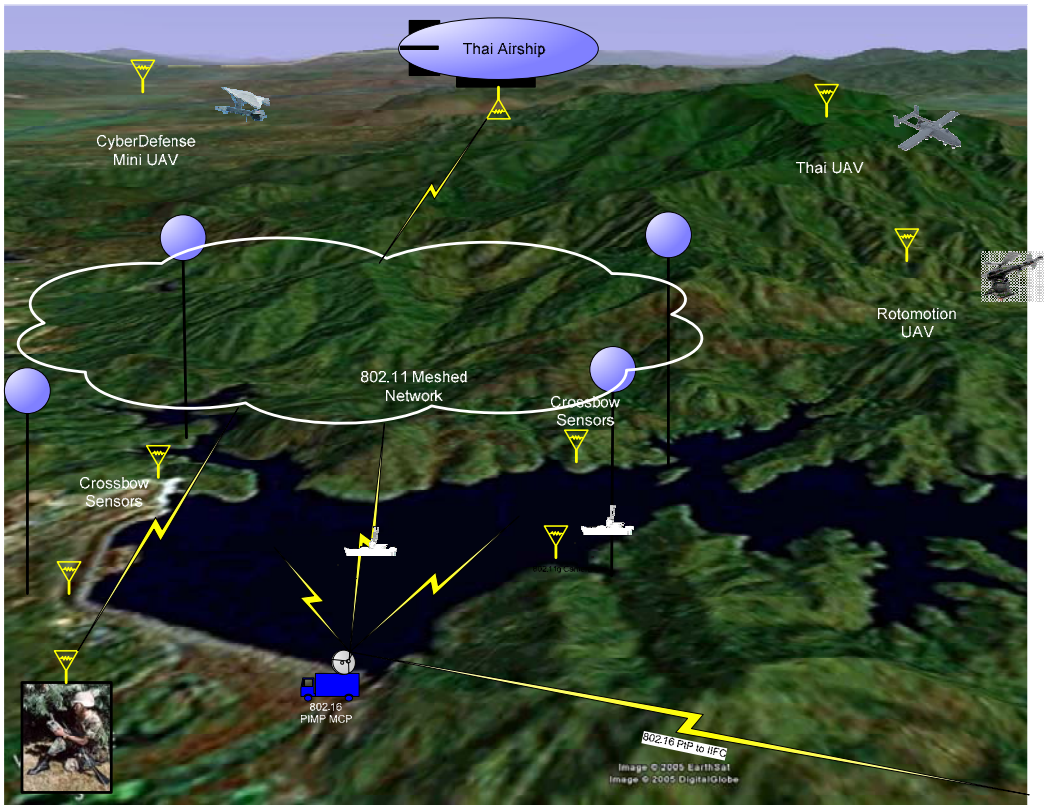


Figure 15. COASTS Demonstration Configuration

3.3.4.1 802.11 (2.4 GHz) End-user Tactical Network.

This local area network will be comprised of an 802.11g footprint established via MeshDynamic access points (MD-300) located aloft on four balloons as

well as placed at various ground stations to provide system and network redundancy. This network facilitates the situational agents end nodes and will connect to a local Mobile Command Platform (MCP) – a Royal Thai Army supplied 10-ton truck equipped with a variety of communications equipment co-located with air assets at the Mae Ngat Dam.

3.3.4.2 802.16 OFDM (5.0 GHz) Backbone.

Four 802.16 OFDM point-to-point suites will be established in order to construct the backbone links from the origination point at the Mae Ngat Dam to the IIFC in Chiang Mai. Three hops will be required which will be accomplished through the mounting of 802.16 suites on cellular towers operated by the AIS Company of Thailand. Ultimately, this will enable an over-the-mountain connection from the JOA to the IIFC.

3.3.4.3 802.16 (5.8 GHz) Maritime Point to Multi-point.

In order to test the functionality of a wireless point to multi-point link to connect two coalition operated security boats, a separate suite of 802.16 OFDM suites will be utilized (on a different frequency than the backbone point-to-point links). The MCP will operate an omni-point antenna linking to two separate omni antennas linked to the planned small boat FLAK.

3.3.4.4 Integrated Crossbow Sensors.

Via an integrated sensor network supplied by Crossbow Systems, Inc, the remote detection portion of the network topology will be tested. The Crossbow family of transceivers utilizes the IEEE 802.15.4 protocol standard for low data rate sensor networks. The network consists of full function and reduced function nodes operating in the 433 MHz, 915 MHz range and 2.4 GHz range. The 2.4 GHz range operates over sixteen channels and uses offset quadrature phase shift keying modulation. The 915 MHz band operates over ten channels and uses binary phase shift keying modulation. Both ranges use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). The nodes can be configured to carry a variety of sensors. The most commonly used is the MTS 310 sensor board which offers an acceleration sensor, magnetic sensor, acoustic sensor, temperature sensor and light sensors.

The Crossbow sensor network provides the capability for self-forming/self-healing sensor grids which are easily deployed. These advantages, combined with small form factor and flexible configuration give today's warfighters a substantial advantage. The creation of integrated sensor/camera networks has applicability in perimeter defense, vehicle security, choke point control and border monitoring. Having the ability to remotely monitor an Area of Interest lessens the burden on the warfighter, allowing for better tactical deployment of human assets. While limited land-based testing of an integrated sensor/camera network has occurred, no current evaluation regarding the performance of this technology in operational environments or littoral waters have been conducted. However, deploying the sensors along a beachhead, the banks of a river, or along piers is well within their current capabilities. The goal is to

provide a low cost yet effective sensor mesh to improve Persistent Intelligence, Surveillance, and Reconnaissance in support of Tactical Coalition Networking Environments.

3.3.4.5 Wearable Computing.

NPS and RTARF personnel shall be equipped with wearable networked computing devices supplied by Mercury Data Systems (MDS). These devices will serve as nodes on the network and personnel will deploy to the surrounding areas at the Mae Ngat Dam to ascertain vegetation effects on signal performance. 802.11g handheld computers will also be utilized to measure COTS capabilities concerning this equipment.

3.3.4.6 Thai UAV.

The RTA or RTAF may potentially supply a UAV, pilot, and associated C2 platforms to support the COASTS project. The Thai UAV, with a maximum range of 200km, will operate at the Mae Ngat Dam and will be equipped with a camera and an 802.11g network connection. The Thai UAV may also provide a live video feed to the MCP and the IIFC.

3.3.4.7 Thai AU-23 Aviation 802.11g Link.

The RTAF will supply an AU-23 fixed wing aircraft and pilot. The AU-23 will operate in the JOA and will be equipped with payloads consisting of various video and wireless networking. The AU-23 will provide an opportunity to test these payloads under varying conditions and altitudes and also to serve as a back-up aerial node in the COASTS network topology.

3.3.4.8 Shared Situational Awareness (SSA) Agents.

These are the nodes and software associated with unmanned sensors such as seismic monitors, sound sensors, and streaming ground or balloon originating video feeds (some with GPS enabled systems). MDS will cooperate with various NPS students, enabling the development of a common information environment through the use of SSA software entitled "C3Trak."

3.3.4.9 Tactical Operations Center (TOC) / Network Operations Center (NOC)

The TOC and NOC will collect and display the data feeds from the various network nodes. This is the C2 center where the deployed technology data feeds are fused and the force multiplying effects of the technology is leveraged. The MCP shall function as a TOC and NOC respectively.

3.3.4.10 SATCOM link.

The RTAF is investigating the feasibility of a SATCOM link between the MCP and the IIFC/Wing 41 to provide for an entirely wireless, large coverage area

network, as well as a secondary communications link for the real-time information display to RTAF HQ, the Maritime Intelligence Fusion Center (MIFC), and NPS.

3.3.4.11 Network Defense.

A survey of the network from a defensive aspect, using open source and COTS products, may be conducted on a not-to-interfere basis. The 2006 COASTS deployment will also utilize a Network Security Detachment, who will establish Computer Network Defense (CND) applications to counter simulated adversary actions, conducted by the Joint Information Operations Center (JIOC) Red Team.

3.3.4.12 Modeling and Simulation.

Using modeling and simulation techniques, empirical results from the demonstration may be compared to predicted results in order to refine modeling capabilities and better predict the data from network testing. The Operations Research department at NPS has conducted war-gaming efforts based on the COASTS interdiction scenario involving realistic small-scale conflicts with UWSA forces attempting to smuggle yaa baa products across the Thai-Burmese border.

3.3.4.13 Micro/Mini UAVs.

Both the RTARF and U.S. military forces are interested in tactical application of UAVs, specifically with respect to the implementation and operational use of micro- and mini-UAVs. These extremely small form factor UAVs, using swarming technologies or other processes, can augment and/or potentially replace the larger, traditional UAVs and manned aircraft. One fixed-wing mini-UAV, one rotor-powered mini-UAV, and one shifting multi-environment micro-UAV will be integrated into the COASTS network.

3.3.4.14 High-Altitude LTA Platforms.

Again, both the RTARF and U.S. military forces are pursuing the application of high-altitude, steerable, non-tethered airships. The Royal Thai Navy (RTN) and Thai Department of Research and Development Office (DRDO) has already begun experimentation in this technology area and is seeking to partner with NPS to provide better, more capable, solutions. The RTN and DRDO will contribute a LTAV to the COASTS 2006 network and NPS will supply four 802.11g network extending balloons to establish aerial communications.

3.3.4.15 Maritime Missions.

The Thai DRDO has previously conducted ship-to-shore wireless network experiments in the Gulf of Thailand and is seeking to link information collected from

seaborne sensors with a surface search radar system deployed to the Thai Naval Station at Sattahip. Ultimately the COASTS 2006 effort will contribute to the Thai objectives as maritime data will be collected, fused, and disseminated to appropriate C2 centers.

In addition, Lawrence Livermore National Labs (LLNL), the NPS, and the MDP-RG are all conducting various field experimentation as part of the Virtual Test Bed concept, which when augmented by the COASTS 2006 demonstration, will showcase the functionality of a fused intelligence-sharing capability for countering asymmetric threats in the maritime environment.

3.3.5 COASTS Critical Event Schedule.

The table below depicts a high level schedule of critical events for the COASTS project - included are the critical development and demonstration milestones.

Date:	Event:
2005	
4-7 October	Concept Development Conference (Monterey)
20-30 November	Site Survey (Chang Mai, Thailand)
5-9 December	Integrated Network Test I (Pt Sur, California)
2006	
1-12 January	Mini-tests (Monterey, California)
12-16 January	Baseline Node Tests (Fort Ord, California)
23-27 January	Mid-Planning Conference (Thailand)
6-10 February	Integrated Network Test II (Pt Sur, California)
20-24 February	Final Planning Conference (Thailand)
20-31 March	COASTS Network Set-up Deployment (Thailand)
22-31 May	COASTS Demonstration Deployment (Thailand)
TBD June	COASTS After Action Review (Thailand)

Figure 16. Critical Events Schedule.

3.4 CRITICAL OPERATIONAL ISSUES (COIS)

- The COASTS project demonstration in Thailand has four primary overarching COIs:
  - Does COASTS provide threat warning information as part of a wireless LAN/WAN?
  - Does COASTS meet performance requirements when deployed to Thailand (ground/jungle/maritime scenario)?
  - Does COASTS enable a last mile data connection for regional and global fusion centers?
  - Can the COASTS network be utilized to enable coalition law enforcement and military operations in a hazardous tactical environment?

The COASTS Oversight Group will refine and finalize the supporting Measures of Effectiveness (MOEs) and Measures of Performance (MOPs), linked to specific operational tasks, standards and conditions, based on the OPORDS for each specific demonstration. The assessment strategy and the final assessment criteria will be clearly delineated in the appendix of the final demonstration OPORD.

3.5 MEASURES OF EFFECTIVENESS (MOE) AND MEASURES OF PERFORMANCE (MOP).

In order to make logical decisions and choices in network development, criteria to measure the value or relative importance of aspects of the network is required. This is an essential pre-requisite for system analysis and predictive study. Both the client (customer, user) and network designer have such measures, and these measures are related.

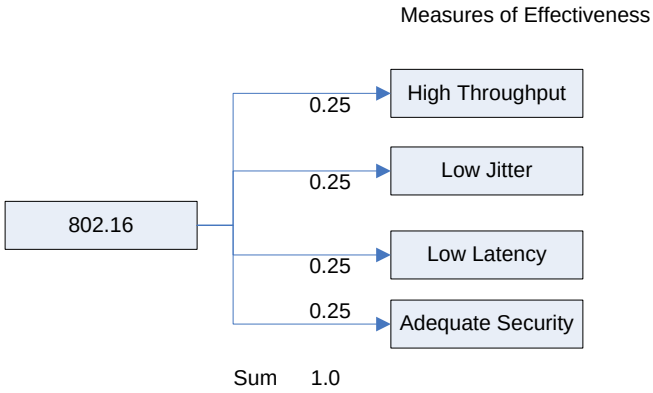
MOE represent the user view, usually annotated and of qualitative nature. They describe the customers' expectations of functional performance and should be viewed as the voice of the user.

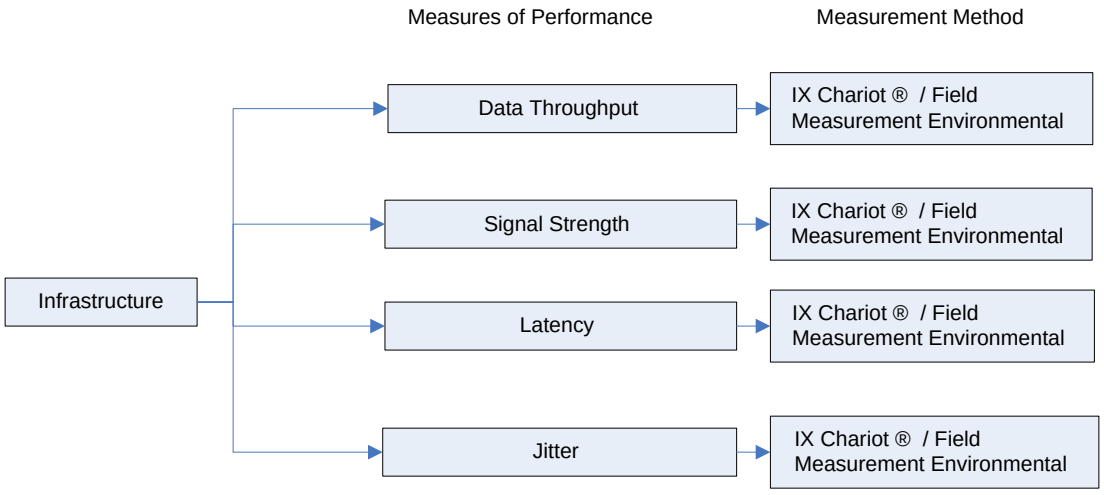
MOP are the corresponding view of the designer; a technical specification for a product. Typically MOP are quantitative and consist of a range of values about a desired point. These values are what a designer targets when designing the network, by changing components, protocols and infrastructure locations, so as to finally achieve the qualities desired by the user.

Both the MOE and the MOP can be constructed as a hierarchy diagram. Each horizontal level of the hierarch represents 100% of the effectiveness or performance.

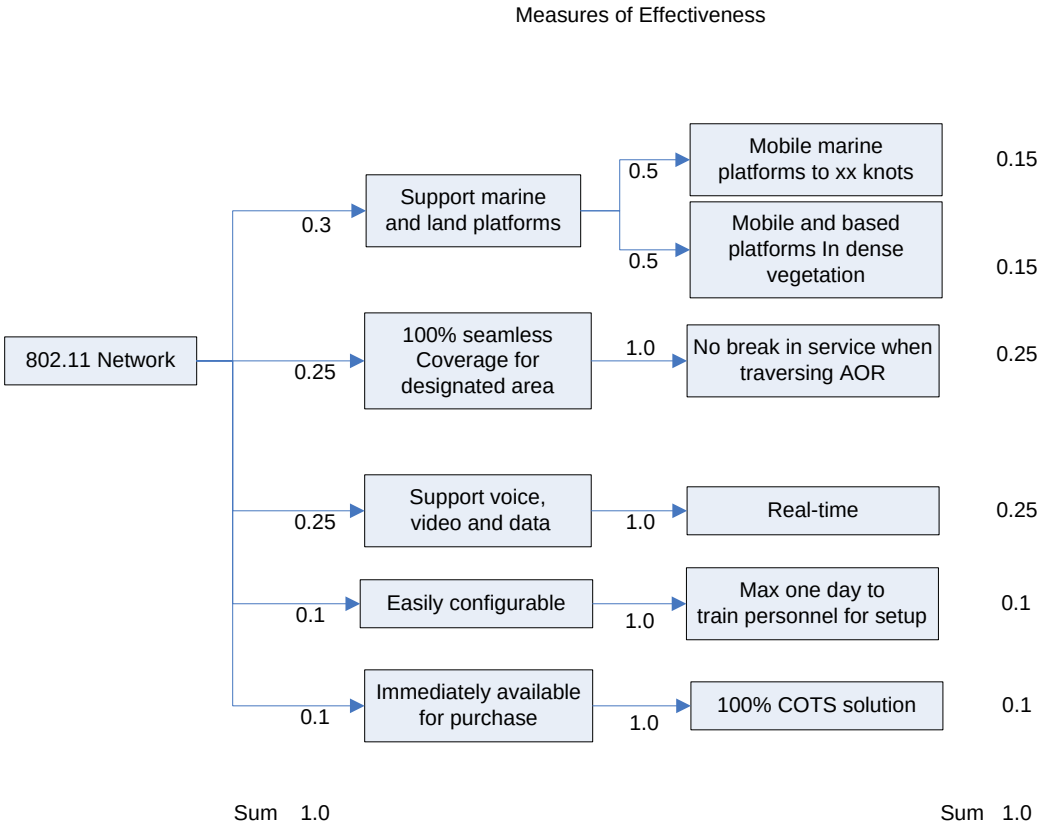
COASTS MOE and MOP were evaluated by the Data Collections team to most efficiently gather and analyze the data associated with each measure. In the following hierarchy diagrams, each node is identified and MOE and MOP are listed in an attempt to specifically communicate each node's data collection needs.

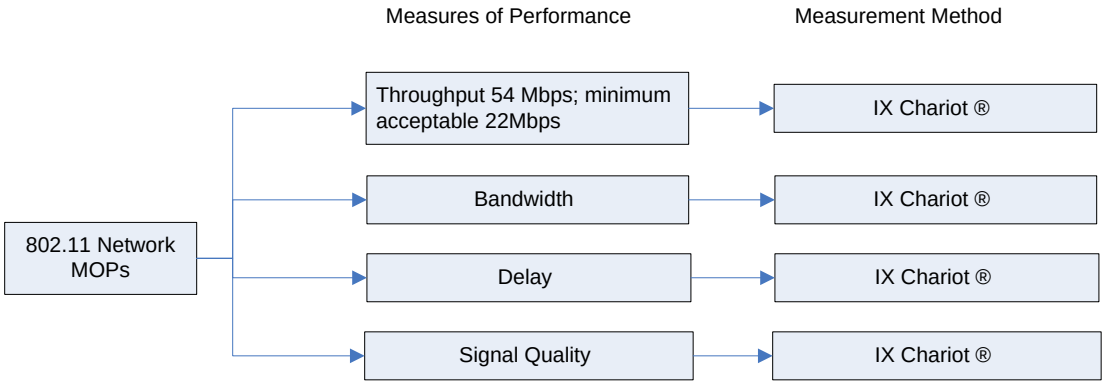
3.5.1 802.16 MOE / MOP



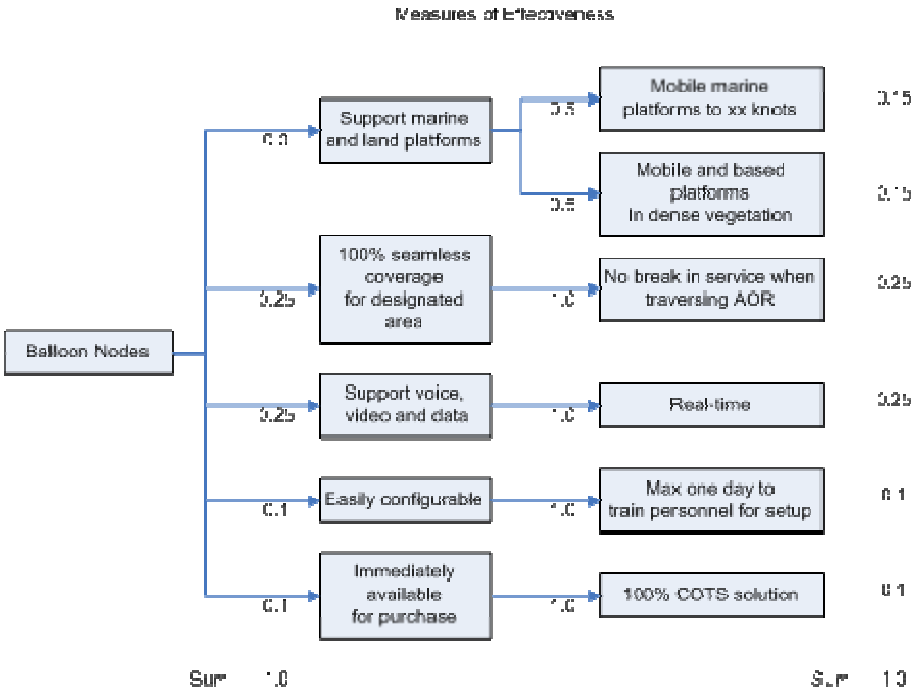


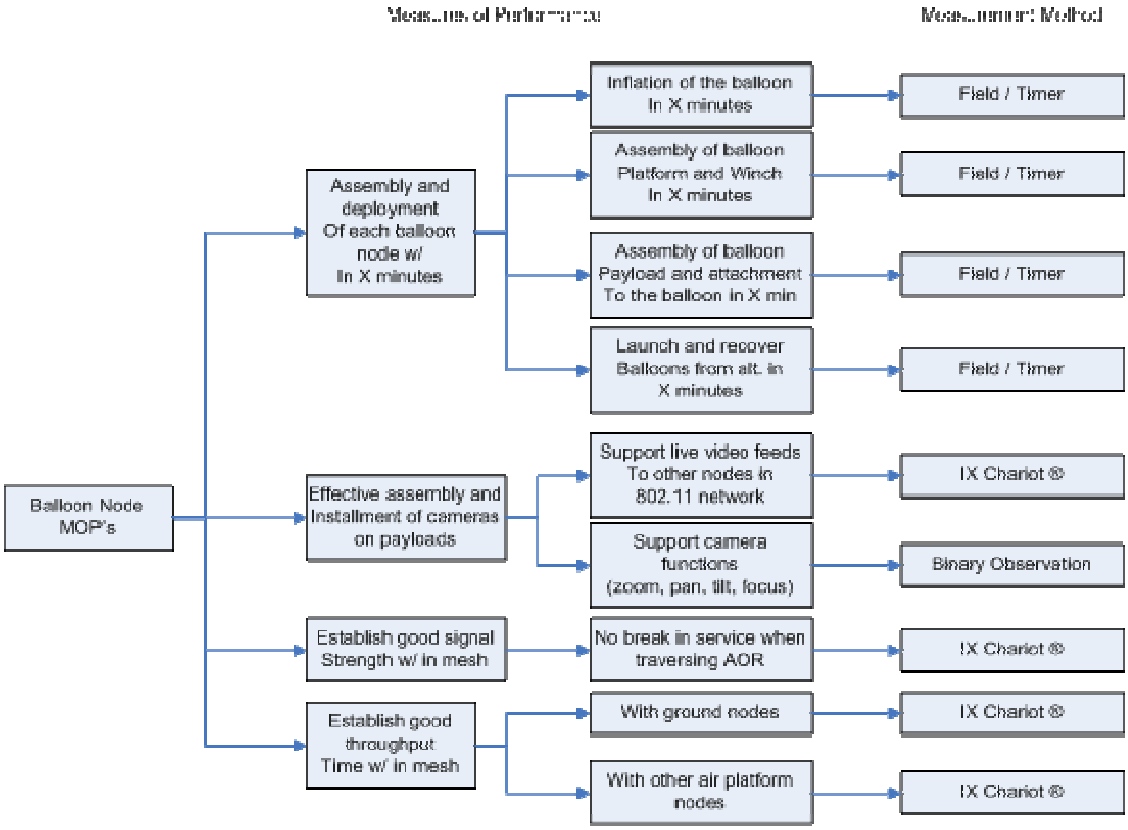
3.5.2 802.11 MOP / MOE



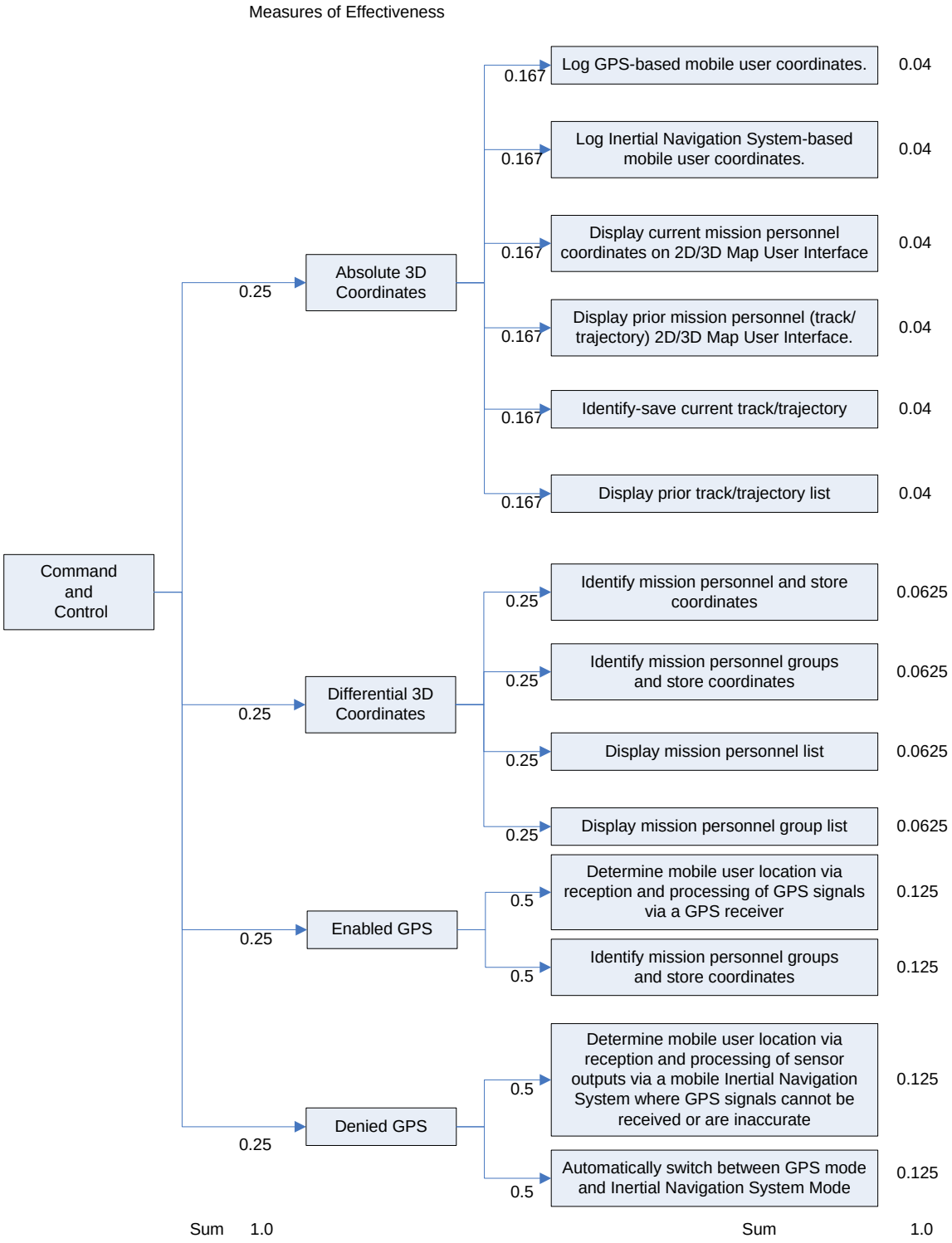


3.5.3 Balloon MOE / MOP

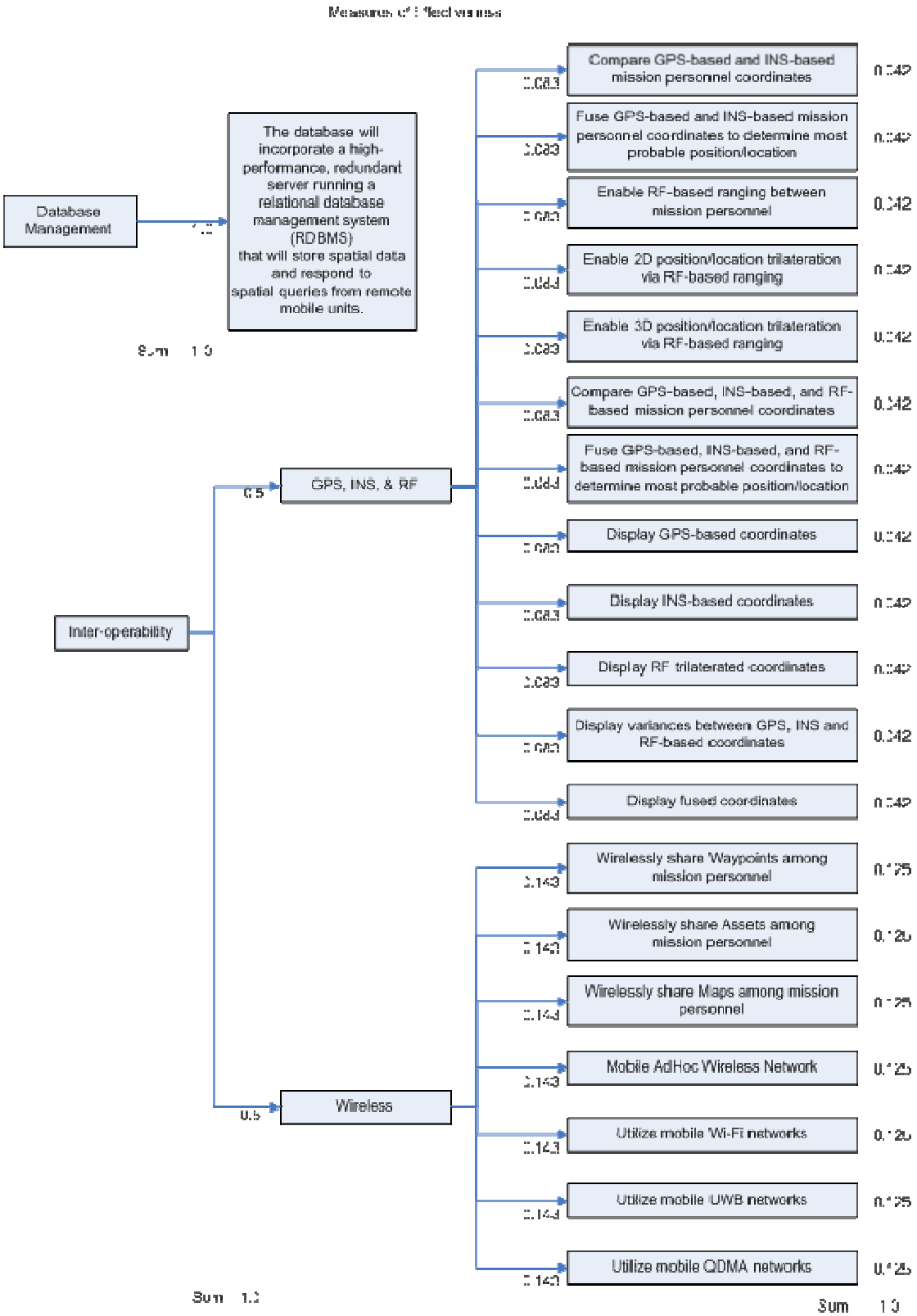




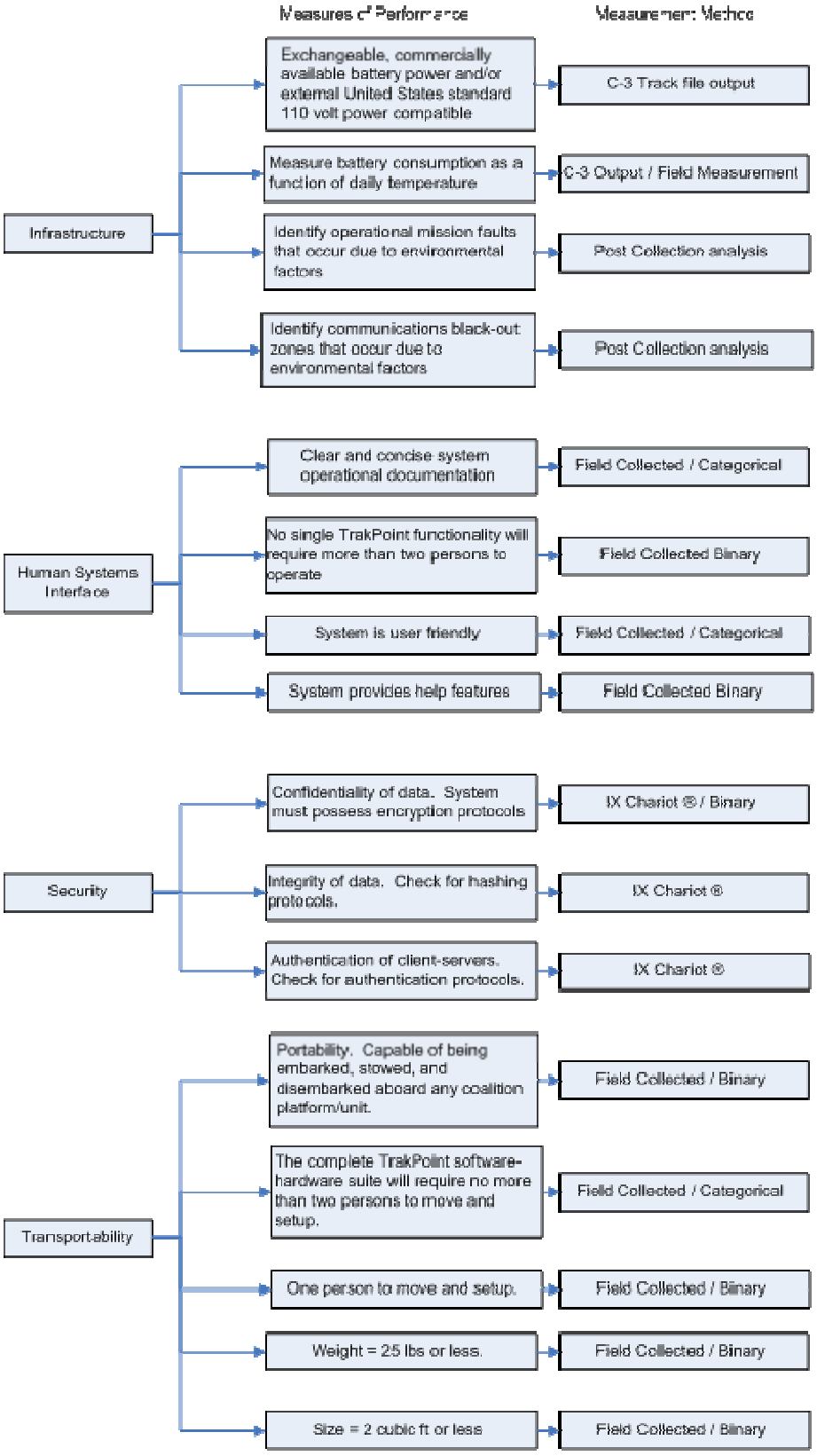
3.5.4 C3 Track MOE -1



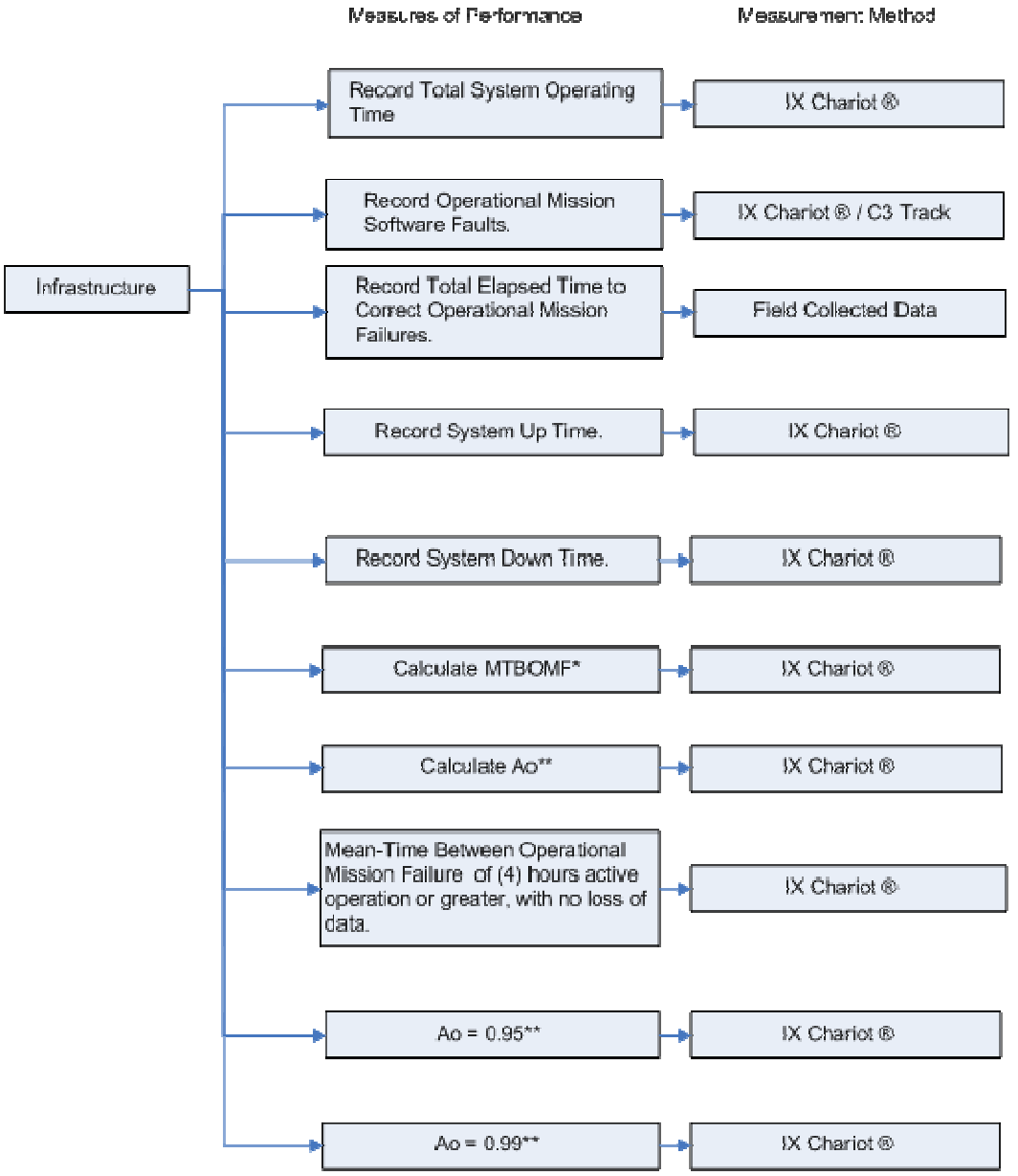
3.5.5 C3 Trak MOE - 2



3.5.6 C3Trak MOP - 1



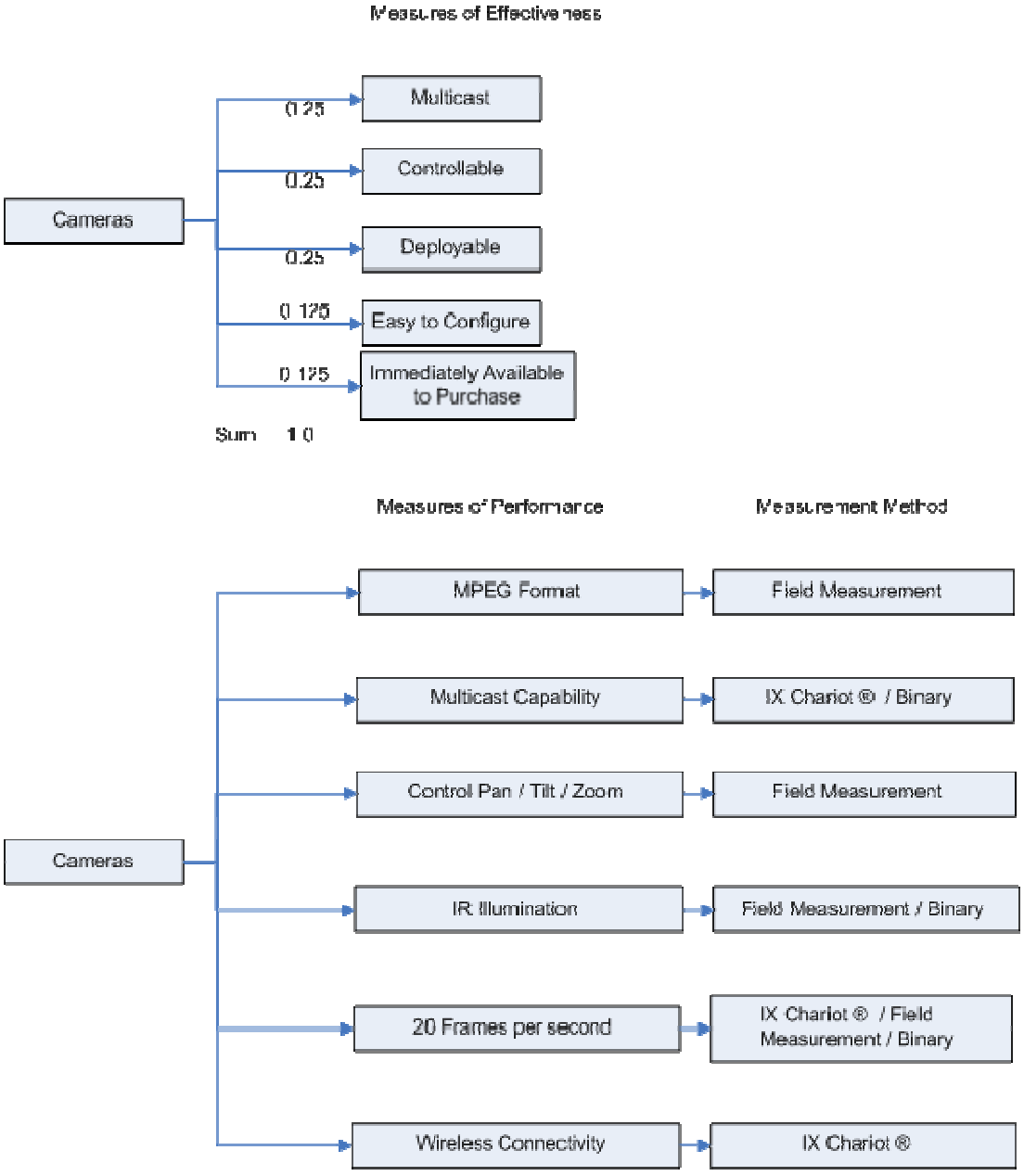
3.5.7 C3Trak MOP-2



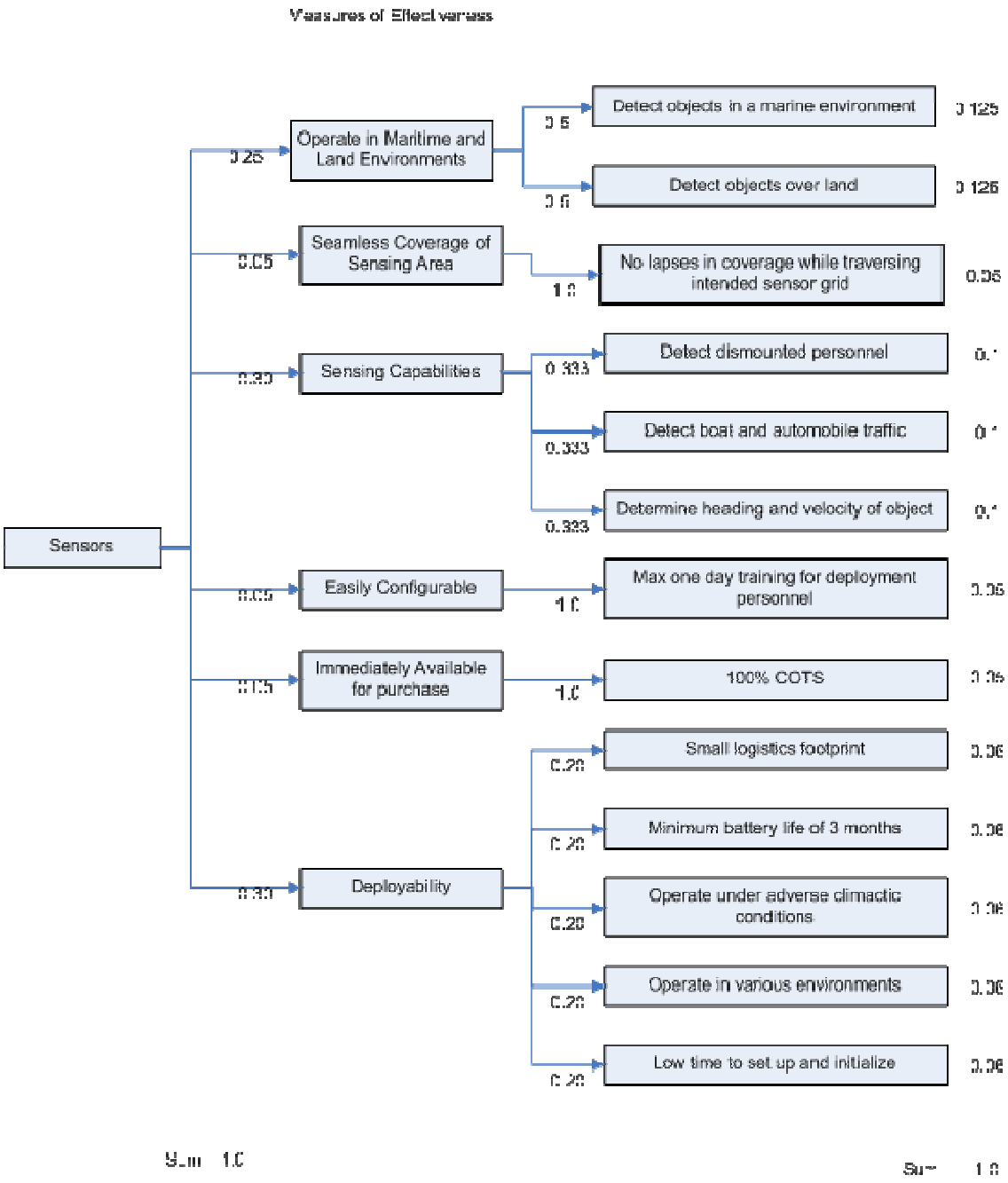
* $\text{MTBOMF} = \frac{\text{Total System Operating Time}}{\text{Number of Operational Mission Software Faults}}$

** $A_o = \frac{\text{Up Time}}{\text{Total Time}}$

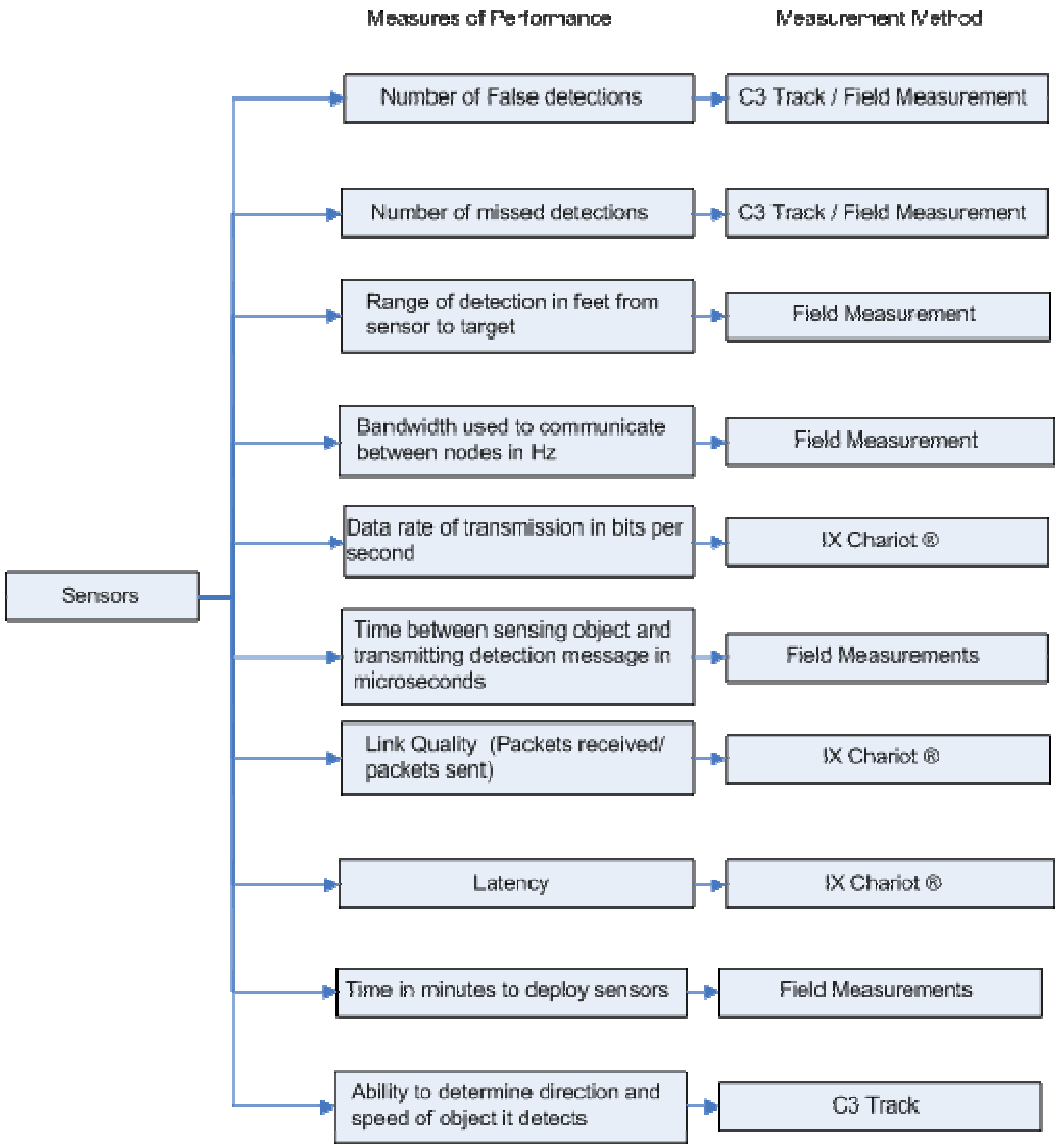
3.5.8 Cameras MOE / MOP



3.5.9 Sensors MOE



3.5.10 Sensors MOP



4.0 MANAGEMENT STRATEGY.

4.1 PARTICIPATING ORGANIZATIONS, ROLES, AND RESPONSIBILITIES.

4.1.1 COASTS Oversight Group.

The oversight committee will be chaired by the NPS Dean of Research. Membership includes the Director MDP-RG, COASTS Program Manager, the COASTS Operational Manager, the COASTS Air Marshall, and the COASTS Student Team and Network Leaders.

4.1.2 COASTS Program Manager (PM).

Lead element of the COASTS project; responsible for project execution, coordination between NPS, DoD, foreign partners, and commercial vendors; responsible for all fiduciary reports and contractual agreements. The COASTS 2006 PM is Mr. James Ehlert (Information Sciences Department faculty member).

4.1.3 COASTS Operational Manager (OM).

The OM is responsible for developing all demonstrations, plans, collection and dissemination of data, site surveys, MOE, MOP, NPS resource allocation, internal NPS coordination, and support to the PM. The OM plans, coordinates and directs all user activities related to the COASTS project. The OM will develop and provide the CONOPS, TTPs, operational mission scenarios, and the overall utility assessment. Additionally, the OM will coordinate administrative tasks for user participants, equipment and facilities supporting demonstration events. The COASTS 2006 OM is Mr. James Ehlert (Information Sciences Department faculty member).

4.1.4 COASTS Technical Manager (TM).

The TM is responsible for technical management including program management, engineering, and acquisition of technologies to integrate and demonstrate. The TM will provide technical support to the OM and manage all funding and technology development efforts related to the COASTS project. The TM has the overall responsibility for establishing criteria for technical performance evaluations. The COASTS 2006 TM is Mr. James Ehlert (Information Sciences Department faculty member).

4.1.5 COASTS Air Marshall.

The COASTS Air Marshall is the authority on all aviation planning, management, and de-confliction. The Air Marshall will liaise with all contractors, Thailand aviation POCs, and all NPS aviation operators. All logistics requiring aviation assets will be managed and controlled by the Air Marshall. The COASTS 2006 Air Marshall is Mr. Ed Fisher (Information Sciences Department faculty member).

4.1.6 Participating Test Organizations.

The primary organization for assessment for the COASTS demonstration in Thailand is the Naval Postgraduate School. Other participating organizations are as follows:

U.S. Pacific Command (USPACOM)
Joint Inter-Agency Task Force West (JIATF-W)
Joint Information Operations Center (JIOC)
Royal Thai Armed Forces (RTARF)
Thai Department of Research & Development Office (DRDO)

4.2 RISK ASSESSMENT, MANAGEMENT AND MITIGATION.

Overall risk is estimated to be low to medium for the COASTS May 2006 Thailand demonstration. Risks can be mitigated by either reducing or adding additional experiments as appropriate. The table below depicts the NPS developed risk matrix:

Risk Area	Rating	Mitigation Approaches
Technology	Low Medium	- early/continuous coordination with partners - early prototyping - multiple data collection events - modeling and simulation - in-process reviews
Schedule - Technical	Low Medium	- schedule estimates based on technology provider agreements - schedule estimates COASTS 2005 lessons learned
Schedule - Demos	Low Medium	- incremental demonstrations - identify/leverage existing events
Assessment	Low	- Individual researchers develop MoE and MoP for their components of the demonstration.
Funding	Low	- significant funding confirmed, additional sponsors contacted

Figure 17. Risk Matrix

4.3 DEVELOPMENT STRATEGY.

The appendices of this document will provide specific guidance on each particular area, element, and component under study during the COASTS demonstration.

5.0 TRAINING, LOGISTIC AND SAFETY.

5.1 TRAINING.

A primary goal of the COASTS project is to execute operational demonstrations in conjunction with U.S. and Thailand forces/resources. Accordingly, appropriate training materials will be developed for each demonstration and operator training will be conducted prior to each demonstration. Training will be performed by a combination of contractor and government personnel. There are also significant hands-on educational opportunities for NPS students, and it is expected that multiple NPS masters theses will be generated by participating US and foreign NPS students.

5.2 LOGISTICS.

Maintenance and logistics support will be conducted using a combination of contractor support and in-house NPS expertise and facilities. This includes the development and distribution of maintenance, training, and operating manuals, instructions, or materials. During the demonstrations reliability, availability, and maintainability information will be collected for later analysis and review.

5.2.1 COASTS Set-Up and Demonstration.

The COASTS team members will transit from Bangkok to Chiang Mai via civilian air transport. All COASTS equipment will be transported from the Bangkok International Airport to the Wing 41 RTAF air base via a RTAF-supplied C-130 or ground transport vehicle. The departure and return schedule are currently not determined but will be based upon operational and administrative requirements during each set-up or demonstration time period. NPS thesis students will handle the logistics, financial management of transportation, as well as necessary host nation support issues.

5.2.2 COASTS Equipment Shipping and Storage.

The NPS will provide JUSMAGTHAI (POC: Lt Col Mel Prell) and the American Embassy Bangkok (POC: LTC Mike Creed) with a list of equipment to be shipped in support of the March set-up and the May demonstration. JUSMAGTHAI will help with the arrival of the equipment and facilitate processing through Thai Customs to minimize delays.

All COASTS equipment will be stored at either Wing 41 or at JUSMAGTHAI. The minimum requirements for either of these facilities will be controlled access (lock and key) to prevent the loss of equipment and air-conditioning to preserve the material condition of electronic devices.

5.3 SAFETY.

The potential exists for safety or environmental hazards associated with technologies being utilized. As needed, a safety analysis will be performed to identify potential safety hazards and risks and determine appropriate controls to preclude mishaps

and reduce risks. This is especially true with regard to manned and unmanned flight operations. The OM will coordinate all safety efforts associated with demonstrations, with the assistance of the Air Marshall for flight operations (see next paragraph).

Air-space management will be handed by the COASTS Air Marshall (Mr. Ed Fisher). Separation of the numerous aviation assets will ensure no collisions occur during field experiments in Point Sur and at the Mae Ngat Dam. An NPS student is designated as the COASTS 2006 Safety Officer, and will conduct all operations under the direction of U.S. Navy Safety Instructions. An Operational Risk Management (ORM) Matrix will be developed and adhered to during all operations.

6.0 MODIFICATIONS.

This CONOP is intended to be a living document. It will be updated as required to reflect changes to the COASTS project as it pertains to the Thailand demonstration. Most modifications will be at the discretion of the COASTS Oversight Group who will approve any substantive alterations to include changes in objectives, funding, schedule, and scope. Any changes which materially affect commitments made by Thailand will be approved by the affected organizations.

APPENDIX A. NETWORK TOPOLOGY

A. INTRODUCTION AND BACKGROUND

1. The goal of the COASTS network is to build and demonstrate the flexibility, mobility, durability, and scalability of COTS 802.11 a/b/g and 802.16 wireless networks deployed to rugged and varied terrain under adverse climatic conditions. These networks will be the infrastructure for transmitting state of the art sensor and ISR data providing improved tracking of littoral and ground movements, identifying which tracks are potential threats, prioritizing them for action, and providing engagement confirmation and battle damage assessment.

2. The COASTS network is designed to be robust, rapidly deployable, modular, and reconfigurable to meet all the needs of tactical, operational, theater, and strategic decision makers in coalition environments. COTS technologies, in particular open standard/open source technologies, provide these capabilities due to their ease of configuration, small form factor, technological proliferation, and low cost separate from the DoD acquisition bureaucracy.

B. 802.16 POINT TO POINT LONG HAUL COMMUNICATIONS SUITE

1. The 802.16 point-to-point links will provide long-haul connectivity between the scenario network at the Mae Ngat Dam and the IIFC in Chiang Mai, Thailand. The 802.16 technology was chosen for integration in the network due to its advantages over the alternative technologies for long-haul communications, namely 802.11, commercial SATCOM (COMSATCOM), and terrestrial (802.3) infrastructure. Specific advantages of 802.16 include:

a. Greater range than 802.11 technologies

b. Higher data throughput rates than COMSATCOM

c. No terrestrial infrastructure required

d. Low cost alternative to COMSATCOM and terrestrial communications

2. Product Information

a. Redline Communications Pre-IEEE 802.16 Compliant Products:

i. AN-50e

- Point to point suite consisting of two base stations, two radio transceiver, and two parabolic flat panel antenna of various sizes.

- Provides high data throughput (up to 54 Mbps) rates with very low latency or jitter at ranges of up to 30 KM.

C. 802.16 POINT TO MULTI-POINT MOBILE COMMUNICATIONS SUITE

1. The 802.16 point to multi-point communications suite will provide mobile connectivity to maritime assets on the Mae Ngat Reservoir. The 802.16 technology was

chosen for integration in the network due its superiority over other wireless technologies for mobile and multipoint wireless networking. Specific advantages include:

a. Client stations associate with only one master station. Clients do not need to constantly re-associate with "in range" access points as is the case with 802.11 coverage.

b. 802.16 communication protocol allows for high relative velocities between master and client stations; 802.11 does not have this capability.

c. Greater range than 802.11 coverage.

2. Product Information

a. Redline Communications Pre-IEEE 802.16 Compliant Products

i. ST-58E

- Man portable client station 802.16 point to multi-point networks.

- Provides high data throughput rates (up to 54 Mbps) to mobile clients at speeds up to 150 Kts.

ii. Point-to-Multipoint configured AN-50E

- Same technology as the PtP AN-50. It includes a special firmware installation that enables routing to multiple slave stations.

D. 802.11 WIRELESS MESHED NETWORKS

1. The Wi-Fi network provides connectivity for mobile clients both on the ground and in the air. Wrapped in a lighter package than other technologies, 802.11 provides the throughput required to utilize various commercial technologies such as VoIP, real-time video, as well as sensor to shooter and intelligence collection data.

2. The 802.11 mesh network technology was chosen for its advantages over alternate methods of wireless local area networking technology such as conventional 802.11, 802.16, and analog radios. In addition, the proliferation of 802.11 enabled clients makes the use of an 802.11 network almost mandatory. Specific advantages of 802.11 mesh networks include the following:

a. It is self-forming and self-healing unlike conventional 802.11.

b. It has higher throughput, lighter pack weight and lower power consumption than analog radios

c. It has a smaller form factor than 802.16.

3. Product Information

a. Mesh Dynamics MD-300 Series

b. Specifications

- 2.4GHz Structured MeshTM backhaul

- Self-healing and self-forming

- Session-persistent roaming
- Integrated 802.11 b/g access
- AES-CCMP encrypted backhaul
- WPA (Personal and Enterprise) security
- Multiple-SSIDs with 802.1q VLAN support
- Independent Security profile per SSID
- Remote Management and Monitoring
- Power over Ethernet
- NEMA rated outdoor enclosure

E. COMMERCIAL SATELLITE COMMUNICATIONS

802.16 point-to-point and point-to-multipoint will be employed to provide long-haul data transmission link from the mesh-network to the IIFC. Satellite transmission will provide connectivity between regional fusion centers located at Bangkok, Thailand and California, USA. Commercial satellite connectivity will serve as an internet gateway to the World-Wide Web.

F. SHARED SITUATIONAL AWARENESS APPLICATION

1. C3Trak (see Figure 18 next page) serves as a mobile, distributed and networked personnel management system that delivers situational awareness capabilities in support of military and law enforcement operations. C3Trak aggregates, processes and displays navigational, environmental, and asset management data, in near real-time, to facilitate C2 decision-making, and the generation and publishing of plans and orders. C3Trak is comprised of three tiers of applications connected through a high speed wireless local area mesh network, and a high speed wireless long-haul wide area network backbone. Military/law enforcement utility of C3Trak involves surveillance and tracking and search and rescue mission areas, but C3Trak can be applied to a number of different mission areas where mobile ad-hoc networking is required. local commander the situational awareness needed to be able to act and react decisively.

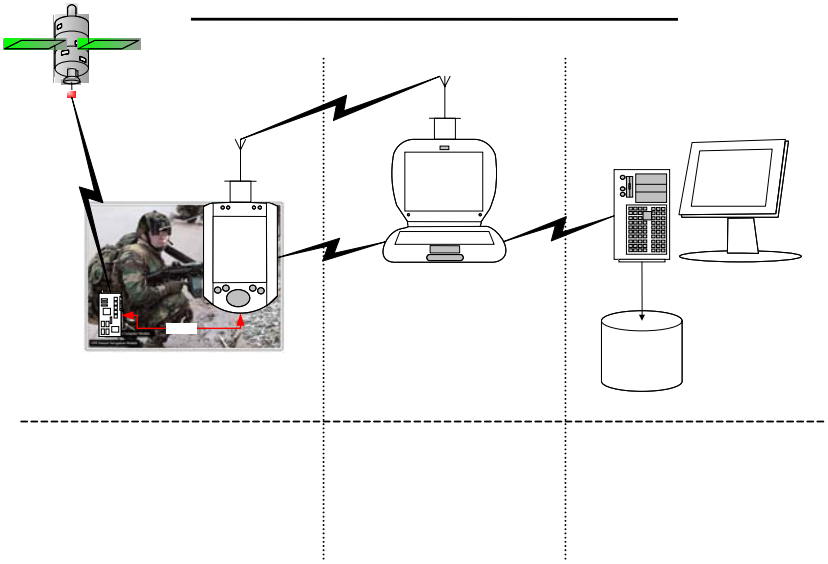


Figure 18. C3Trak System Diagram

2. The 1st tier establishes a peer-to-peer network of mobile handheld devices, linked to sensors that provide navigational inputs. The 1st tier handheld clients can operate both in GPS enabled and GPS-denied environments, and can be configured to automatically switch between modes of operation. In GPS-denied environments, sensor inputs to the mobile clients are provided by quadrature multiple frequency ranging (QMFR), RF Location Beacons, PNM, etc. Mobile handheld units possess full capabilities to communicate with other mobile clients on the meshed wireless local area network, including the 2nd tier base station unit. Communications include full text messaging capabilities, forwarding of absolute and relative spatial positions (see Figure 19 next page), and asset management of resources, including mesh sensors and monitoring and control of networked imaging devices.

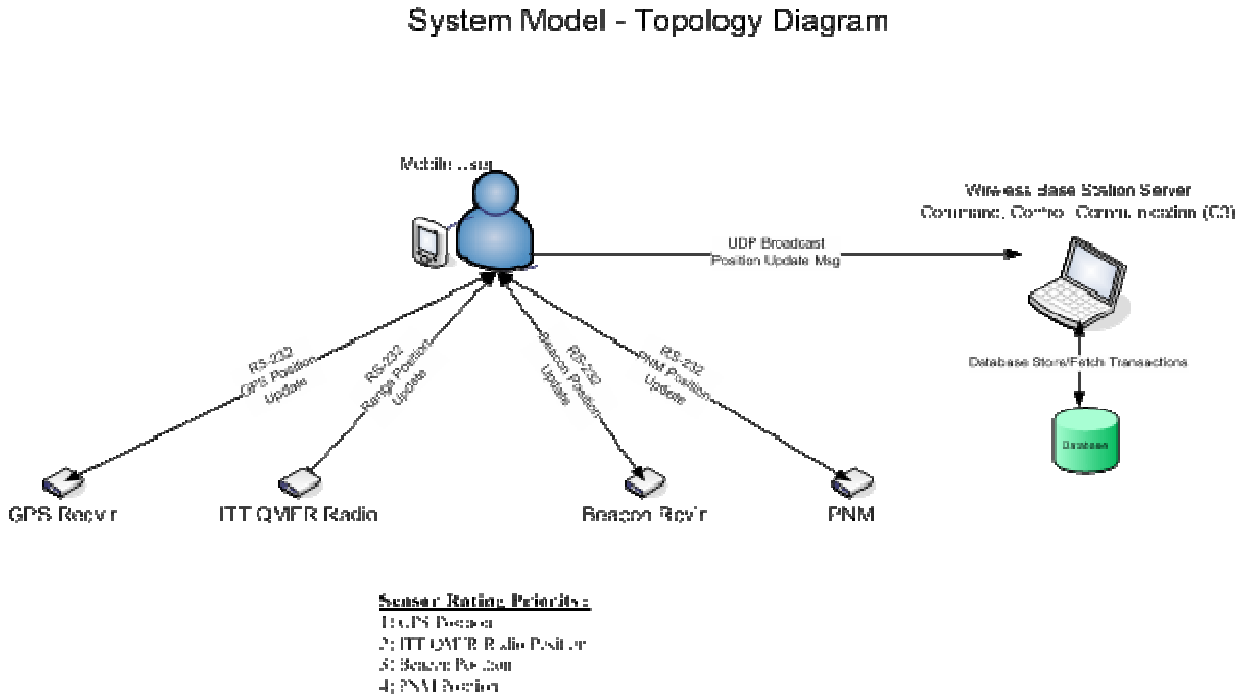


Figure 19. Position sensor integration

3. The 2nd tier base station unit serves as the primary command and control node in the local area network. It provides a near real time common operational picture as it correlates and fuses data from multiple sensors and intelligence sources to provide the local commander the situational awareness needed to be able to act and react decisively. The base station unit acts as the intermediary between the mobile clients and the data warehousing and processing 3rd tier relational database management system. Similar to the handheld mobile clients, the base station unit possesses an extensive suite of integrated automation, messaging, and collaborative applications. However, the base station unit incorporates additional aggregation and processing applications to facilitate the local area commander with mission planning and execution. The 2nd tier feeds aggregated data, by way of a high speed wireless long-haul communications link, to the 3rd tier relational database.

4. The 3rd tier applications incorporate the force monitoring applications required by the regional commanders to effectively assess military operations. It is comprised of a series of redundant relational database and web-host servers, designed to accommodate and process the large volumes of data sent from the local area meshed network

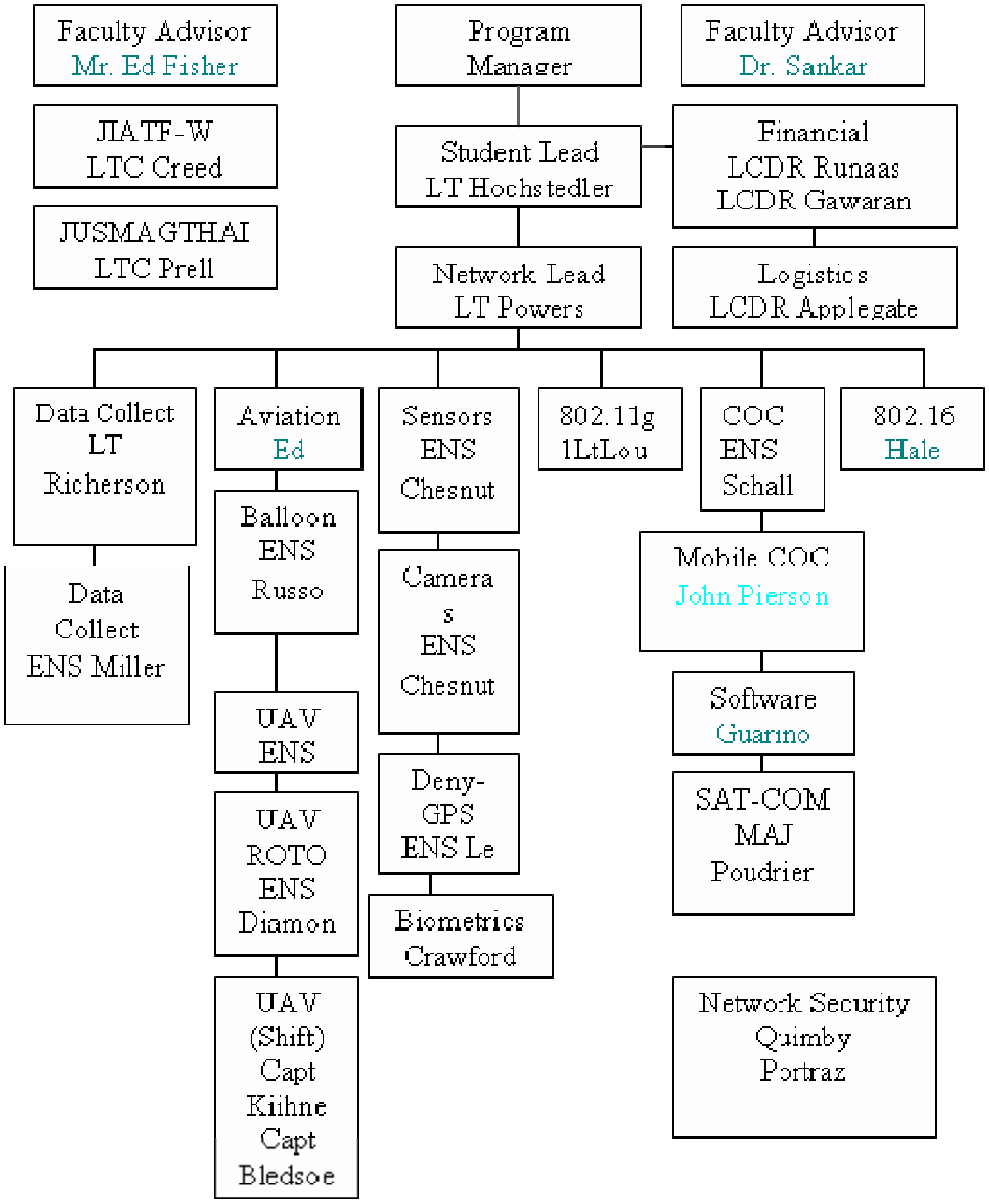
APPENDIX B. COASTS FUNCTIONAL AREAS

Functional Area	Personnel	Description
Project Managers	Mr. James Ehlert Gp. Capt. Teerachat (RTAF) Gp. Capt. Triroj (DRDO)	Guidance and management of overall project goals and operations.
Air Boss	Mr. Ed Fisher	Coordinate and establish overall airspace coordination plan. Manage and be responsible for all platform operations above ground level, to include manned and unmanned aircraft operations within the JOA. Act as Deputy Program Manager to assist PM when not engaged in air activities.
Aerial Balloons	ENS Joseph Russo	Build and establish an operating 802.11g network node as payload on a balloon.
802.11g	1st Lt Robert Lounsbury	Build and establish the 802.11g mesh network
802.16 OFDM point to point	Mr. Ryan Hale	Broaden the connectivity between a common base station and two or more remote locations within a wireless network.
Data Collection	LT John Richerson ENS Red Miller	Manage the collection of all pertinent analysis data to establish recorded findings.
Sensor Grid	ENS Michael Chesnut	Establish network monitored sensors comprised of GPS, video, audio, and other sensors.
Video	ENS Michael Chesnut	Establish and manage all video collection assets on the network.
Network Topology	LT Jonathon Powers Mr. Ryan Hale	Define the layer 1 (physical layer) requirements and components for the overall network operations.
Situational Awareness	Mr. Rich Guarino	Interface with COTS providers to establish a situational awareness solution for the COASTS program.
Evaluation	Mr. Robert Sandoval	Monitor and provide networking metrics for the establishment for the COASTS network.

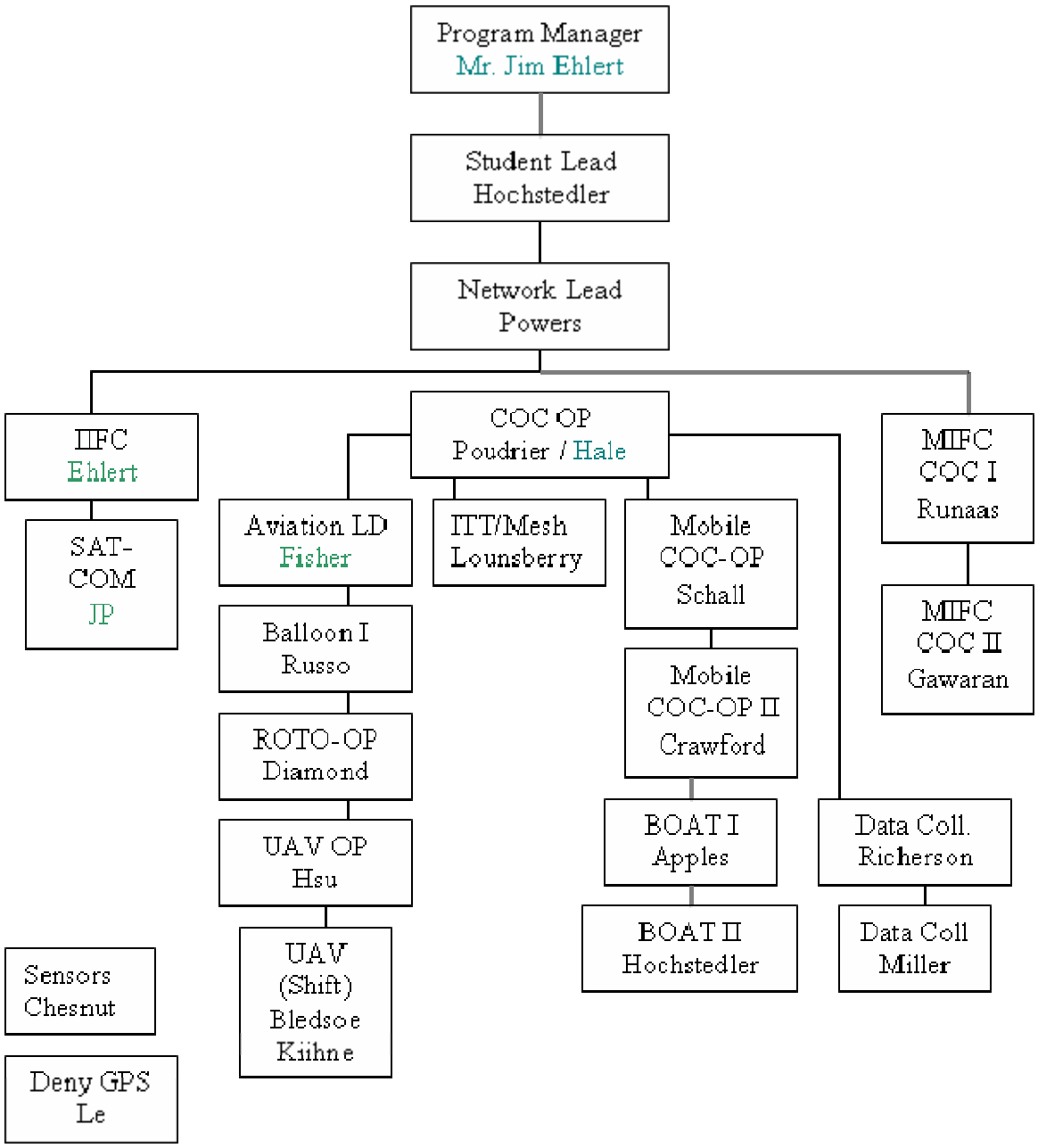
Functional Area	Personnel	Description
Vulnerability Assessment	LT Jonathon Powers Mr. Ryan Hale	Define, establish, and provide solutions for the critical network vulnerabilities.
Weather	LT John Richerson	Monitor and provide meteorological information for further correlation to network operating characteristics.
COC	ENS Stephen Schall	Build and operate a command center in which to coordinate all network operations.
SATCOM	MAJ Joel Pourdrier	Build and establish a SATCOM link to show portable link capability.
Strategic Node	LCDR Kris Runaas LCDR Ed Gawaran	Manage the Strategic Data Link at the receive node at the Alameda, CA USCG Data Fusion Center.
UAV (fixed wing)	ENS Michael Hsu	Manage and control the Cyberdefense micro-UAV: Cyberbug. Establish Network link to the UAV.
UAV (rotary wing)	ENS Scott Diamond	Manage and control the Roto-motion micro-UAV. Establish Network link to the UAV.
UAV (kite)	Mr. Ryan Hale	Manage and control the helia-kite network extender.
Deny GPS	ENS Phong Le	Manage and establish the Deny GPS technology to establish node testing.
UAV (MMLAV)	Capt Josh Kiihne Capt Drew Bledsoe	Build, manage, and establish the transformable micro-UAV. To include the network connection to the UAV.
802.16 OFDM point to multi-point maritime link	LT Rob Hochstedler	Build FLAK in order to establish an over-water 802.16 maritime security link.
802.11 Backhaul	ENS Stephen Crawford	Test and support the 802.11 deployment.

APPENDIX C. NPS THESIS RESEARCH IN SUPPORT OF COASTS 2006

LT Hochstedler	Wireless Network Topologies ISO countering Asymmetric Threats in the Maritime Environment
LT Powers	Data Compression Applications in deployed Wireless Networking
ENS Chesnut	Applications of Integrated Sensors for Tactical operations
LT Richerson	Optimization studies for the Usage of Micro-UAVs in a Tactical Environment
ENS Le	Deny GPS in tactical wireless environments
LCDR Runaas LCDR Gawaran	IT Costs of deploying Hastily Formed wireless networks into tactical theatres of operation
ENS Diamond	Use of wireless networks ISO fire-control data passage to Strike Operations
ENS Russo	Deployment of Lighter than air vehicles in tactical wireless network deployments
ENS Hsu	Deployment of micro-UAVs for support of ISR in tactical environments
1st Lt Lounsbury	Deployment of 802.11g wireless networks ISO tactical operations
MAJ Pourdrier	Analysis of UAV-received intelligence in combat operations
Capt Kiihne Capt Bledsoe	Design and analysis of a transformable mini-UAV
LCDR Keith Applegate	Analysis of Logistical requirements for deploying wireless networks
MAJ Quimby Maj Potraz	Wireless Network Security in Tactical Network Deployments
ENS Crawford	Study of 802.11 backhaul configurations for Tactical Deployments
ENS Schall	Code applications in wireless sensor deployments
ENS Miller	Data Collection in wireless network deployments



COASTS 2006 Personnel Design Matrix



COASTS 2006 Personnel Deployment Matrix

APPENDIX D. DATA COLLECTIONS

A. INTRODUCTION AND BACKGROUND

Validation of hypotheses using collected data is an essential step in the process of research. Be it test and evaluation, proof of concept, or theoretical modeling, the collection and analysis of data provide accepted mathematically rigorous means by which conclusions are drawn. In the context of COASTS, data collection and analysis are a means to empower decision makers to draw conclusions based on data collected in the field for each phase of COASTS 2006.

B. METHODOLOGY

1. Data Collection Points

a. Environmental Data

Based on past observation of network performance in Thailand, it is theorized that network performance is significantly affected by temperature. To validate this hypothesis and potentially model the affects of temperature on network performance meteorological data will be collected in each phase of the COASTS project. For the context of COASTS 2006, distance measurements and locations are also considered environmental data.

b. Benchmarking Data

MOE and MOP inputs primarily drive the need for benchmarking by identifying specific metrics of concern and providing thresholds of acceptable performance. Specific metrics require a trend of performance across a specified range that can only be evaluated against preliminary, or benchmark data. Still other metrics require specific performance thresholds at all levels of effective use.

Data collected before the Thailand phase of operations provides a pool of data collected in known conditions to compare to data collected in the operational phase. Also, initial conclusions and potential areas of interest may be generated through the analysis of this initial data. The data also provides a means to analyze the performance of sensor systems and network hardware against the claims of the manufacturers.

Examples of benchmarking are the observed rate of detection at given distances for a specific sensor or the observed signal strength generated from a specific antenna at given distances.

c. Network Data

Performance of computing networks is potentially affected by a wide and varied array of inputs and atmospheric conditions. Signal strength, latency, throughput, packet loss, and jitter are just a few of the performance measures associated with network performance. Each of these and additional measures will be collected throughout the project using a commercial application that collects and stores data network specific data.

A time stamp is associated with each data point to match network data with data collected apart from the network.

d. User Data

Subjective data such as ease of use and usability of displayed information will be developed as categorical data. This will enable regressive techniques to be used from which the team can draw more useful conclusions.

e. Data Collection Operations

To the maximum extent possible, data collection will be conducted in a manner that minimizes error. When possible gauge error will be estimated from manufacturer specification and input into the statistical model. Data collection methods will be utilized that minimize the impact on the observed values.

f. Data Preparation / Model Formulation

Once data has been collected, a permanent copy of all raw data will be kept in a central location by the Data Collection node leader. Data normalization and manipulation will only be carried out with copies of the raw data collected.

Statistical models will, to the maximum extent possible, minimize variability while maintaining accuracy and tractability. Construction of statistical models will be documented in such a manner as to assure reconstruction of the model solely from the documentation.

g. Analysis and Conclusions

Only after statistical models have been constructed and validated in accordance with paragraph f. above will any inference from analysis be undertaken.

APPENDIX E. MINI-UAVS

A. INTRODUCTION AND BACKGROUND

Mini-UAVs will be used in the COASTS scenario to provide tactically persistent surveillance/reconnaissance. In the 2006 Thailand field experiment, presence of potential bad actors will be noted by sensor-"triggers", and mini-UAVs will be launched to gain additional information on these bad actors and pass the information to local-tactical, regional-operational, and strategic C2 centers for continued consideration.

B. CYBERDEFENSE CYBERBUG MINI-UAV

The CyberBug is a small, lightweight, scaleable, low-cost mini-UAV. One man may unpack, assemble, and launch the CyberBug in under one minute. It is hand-launched and capable of utilizing an auto-land system. It may be programmed for autonomous operation with manual override available. It is normally equipped with a stabilized gimbaled low light high resolution camera, and an IR camera payload is available. It is electrically powered, and has about 45 minutes endurance.

- Length 25-56 inches
- Wing span 30 inches to 60 inches
- Weight ~ 2.6 pounds scalable to 5 pounds

- 45 minutes to 3.5 hours approximate flight time
- 5-20 MPH
- Autopilot / GPS navigation
- Hand held viewer and joy-stick
- Small 12x camera w/Optional cameras for day and IR(Indigo)
- 9 -18 Volt battery
- Carrying case (small unit)
- EO/IR payload is scalable up to several pounds
- Includes short range data link (long range is option)

C. ROTOMOTION SR-100 MINI-UAV

The Rotomotion SR-100 is a relatively small vertical take-off and landing UAV. It may be programmed for autonomous operation or can be flown manually. It has an auto-land and auto-takeoff capability. It may be equipped with either a day camera or an IR camera, and utilized a low-jitter capability to stabilize the video feed. It may be

gasoline, diesel, or electrically powered. If equipped with the electrical motor (COASTS preference for low-observable operations), it has about 60 minutes endurance.

- 802.11-based Telemetry System
- Length:2250 mm, 89”
- Main Rotor (M/R) Dia.:1900 mm, 75”
- Dry Weight:16 kg, 35lbs.
- Fuel Cap:2 liter, 67 oz. ,(alcohol,diesel,50:1, 2cycle gasoline)up to 14 liter, 470 oz., tanks available
- Engine :2-Stroke gasoline, alcohol, diesel conversion, or electric
- Generator (optional):150W, 12V power bus with battery backup
- Climb rate:122 mpm, 400fpm (AFCS regulated)
- Speed:10 mps, 65 fps (AFCS regulated)
- Endurance:30 min to 2 hours (depending on fuel tank configuration)
- Max Payload: up to 7 kg, 20 lbs (depending on options, altitude, fuel load)

APPENDIX F. COASTS 2006 STORYLINE

The arrival of a longboat suspected of involvement in drug and arms smuggling operations will be detected by various unattended sensor suites deployed at a tactical waterborne choke-point(s). When triggered by the motion of the longboat, the sensors will send an automatic system alert through the C3Trak SSA application. This system alert will be observed by all the tactical forces connected to the network (refer to Figure 2), by the local C2 center (the IIFC in Chiang Mai), by the remote C2 center in Bangkok (RTAF HQ) and finally by the strategic C2 center in Alameda, CA (at the U.S. Coast Guard Maritime Intelligence Fusion Center (MIFC)). The coalition small boat unit will also receive the alert via the 802.16 OFDM mesh network. Coalition small boats, camouflaged as local river merchants, will track the longboat, passing intelligence via Voice-over-IP (VoIP) communications and imagery back via mounted IP cameras over a wireless link.

The system alert will enable coalition operators to track the movement of the longboat through various sensors deployed along the waterway. At a pre-determined trigger point, the tactical C2 center will order the launch of the mini-UAVs and the full-sized UAV to establish tactical persistent surveillance. The UAVs will pass video (electro-optical and infrared) through a wireless network established by four tethered aerial balloons, operating at altitudes up to 3500 feet, and each equipped with a wireless access point, and one non-tethered unmanned lighter-than-air vehicle (LAV) operating at altitudes of up to 10,000 feet. The data obtained from the UAVs will be collected, fused, and disseminated by the C3Trak application to the on-scene commanders in the Mobile Command Platform (MCP).

When the longboat arrives at a "drop-point" (near the end of the reservoir, close by the Mae Ngat Dam Boat Shop) the drug and explosive shipment will be transferred into the cargo bed of two awaiting trucks and an unidentified bad actor (man) is given a CD (contents include the details of the smuggling operation to include financial ties with terrorist organizations). This entire process is being remotely monitored (UAVs and balloons) and displayed at the local, regional, and strategic C2 centers. After the transfer is complete, the longboat departs along the reverse route. A bad actor convoy (two trucks) is tracked as it moves along the road atop the Mae Ngat Dam while the individual bad actor will leave on foot on a northward path.

The scenario will then split into two parts to research, test, and display the versatility and multi-tasking potential of the COASTS network. One part will entail the bad actor being tracked on foot by a Royal Thai Army and Police squad. The bad actor will cross land-based sensor suites, again initiating a C3Trak system-wide alert. The IIFC will order the interdiction squad (equipped with a wearable computing device which can send/receive all network data, and biometric and explosive residue collection capabilities) to coordinate the apprehension of the suspected bad actor.

The second part of the scenario will entail the convoy being tracked by the network sensors simultaneously. The vehicle carrying the larger portion of the drugs will also cross a Guardian sensor grid, deployed alongside the road, sending another C3Trak system-wide alert. At this point, orders will be passed from the strategic command and control center (MIFC), via the operational node in Bangkok (RTAF HQ), to capture all monitored units: longboat, trucks, and bad actor. The bad actor will be captured without incident, but both the longboat and trucks are armed and put up heavy resistance against capture. Both the coalition small boat team and the vehicle interception team pass SITREPS via the COASTS network requesting tactical air support (L-39 jets).

After apprehension of the bad actor is affected, biometric data will be gathered and passed to the MIFC for identity verification. Once positive confirmation is received that the captive is the high value target in question, the coalition ground forces holding the bad actor will pass initial intelligence from the CD (captured with the bad actor's personal effects) and initial custody status via C3Trak to all network users as well as the IIFC and MIFC.

The COASTS Watch Officer (CWO) at the IIFC will request an air strike against the convoy from RTAF HQ. As part of this request the CWO will pass GPS positions and other targeting information. The RTAF HQ directs two L-39s from Wing 41 to conduct the air-to-surface strike.

Concurrently, coalition maritime interdiction teams will apprehend the long boat. After apprehension of the bad actors, biometric data will be gathered and passed to the MIFC for identity verification. Once directed to maintain custody of the bad actors, the coalition maritime interdiction team will pass mission status via C3Trak to all network users as well as the IIFC and MIFC.

The L-39's loiter pending resolution of the maritime interdiction. The scenario will finish after the maritime interdiction is completed and the L-39's have departed the JOA.

APPENDIX G. DISTRIBUTION LIST

1. Mr. James F. Ehlert
   Director, Maritime Domain Protection Research Group
   (MDP-RG)
   Naval Postgraduate School
   Monterey, California

2. Colonel Thomas Lee Williams
   Deputy Science Advisor
   U.S. Pacific Command (USPACOM)
   Camp Smith, Hawaii

3. Mr. Russ Holland, Chief of Staff
   Joint Inter-Agency Task Force West (JIATF-W)
   Camp Smith, Hawaii

4. Mr. Kurt Badescher
   US Special Operations Command (USSOCOM)
   Tampa, Florida

5. Mr. J. Christopher Griffin,
   Westwood Computer Corporation

6. Mr. Ralph L. Boyce, US Ambassador of Thailand
   US Department of State (DoS)
   Bangkok 10330 Thailand

7. Lt Col Mel Prell, USAF
   Joint US Military Advisory Group Thailand (JUSMAGTHAI)
   Bangkok 10120 Thailand

8. Lieutenant General Krita Kritakara
   Deputy Secretary
   Thailand National Security Council (NSC)
   Bangkok. Thailand

9. Lieutenant General Apichart
   Director-General, Defence Research & Development
   Office (DRDO)
   Parkred, Nonthaburi, 11120

10. Group Captain Dr. Triroj Virojtriratana
DRDO COASTS Project Manager
5th Floor A1 Muangthong Thanee
Parkred, Nonthaburi, 11120

11. Group Captain Wanchai Tosuwan
Director, Research & Development Promotion Division
Parkred, Nonthaburi, 11120

12. Group Captain Teerachat Krajomkeaw
Directorate of Operations
Royal Thailand Air Force (RTAF) Headquarters
Bangkok, Thailand

13. Mr. John Laine
Senior Contractor, JIATF-West
Interagency Intelligence Fusion Center (IIFC)
Chang Mai, Thailand

14. Mr. Craig Shultz
Lawrence Livermore Laboratories (LLNL)
Livermore, California

15. Mr. Robert Sandoval
Joint Intelligence Operations Command (JIOC)
San Antonio, Texas

16. John Taylor
President, Mercury Data Systems
Greensboro, North Carolina

17. Captain Phil Erdie, USMC
U.S. Marine Corp Systems Command (MARCORSYSCOM)
Quantico, Virginia

18. Mr. Thomas Latta
C4ISR & IO PM
Space and Naval Warfare Systems Command

19. RADM Nimmick, USCG
Maritime Intelligence Fusion Center (MIFC)
Alameda, California

20. Mr. Jim Alman
President, CyberDefense UAV Systems
St Petersburg, Florida

21. Mr. Dennis B. D'Annunzio
COO, Rotomotion, LLC
Charleston, South Carolina

22. Mr. Curtis White
Commander's Representative
AFRL/XPW – AFFB/CCT
USAF Force Protection Battle Lab
Lackland AFB, Texas

23. Mr. Archie Newell
Cisco Syste23.ms

24. Mr. Mike Rathwell
Identix Corporation
Jersey City, New Jersey

25. Dr. Leonard Ferrari
Dean of Research
Naval Postgraduate School
Monterey, California

26. Dr. Pat Sankar
NPS Distinguished Fellow
Naval Postgraduate School
Monterey, California

27. Dr. Gurminder Singh
Director of the Center for the Study of Mobile Devices
and Communications
Naval Postgraduate School
Monterey, California

28. Dr. Carlos Borges
Mathematics Department
Naval Postgraduate School
Monterey, California

29. Dr. Frank Shoup
Director of Research, Meyers Institute, GSEAS
Naval Postgraduate School
Monterey, California

30. Dr. Dan Boger
Chairman of the Graduate School of Information Sciences
Naval Postgraduate School
Monterey, California

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. COMPLETE EXPERIMENT RESULTS

PIR MAXIMUM HUMAN DETECTION RANGE

Detection Distance (Feet)	Elevation (Inches)	Speed[1]	Time of Day[2]	Temperature (F)	Pressure (inHg)	Humidity
45.3	12	3	6	64.9	30.15	53.3
27.9	3	3	9	75.1	29.76	70.6
35.7	5	1	4	70.6	30.15	33.4
38.4	8	2	16	77	29.97	94.9
42.1	11	2	2	59.3	30.2	51.4
32.6	4	2	13	57.4	30.00	94.1
28.1	2	3	5	54.5	30.12	82.8
35.2	11	3	15	100.7	29.6	23.9
38.5	6	2	8	88	29.80	77.2
25.6	0	1	10	64.9	30.15	53.3
31.4	9	1	7	106.8	29.57	20.3
39.5	7	3	12	41.8	29.62	95.1
38.1	5	2	0	36.4	28.68	93.6
26.2	1	2	14	93.6	29.74	46.7
37.7	8	2	3	81.4	29.88	84.2
39.3	10	1	11	57.6	29.56	85.5
27.5	2	2	1	61.5	29.85	83.6

Note:

1. Speed categories are defined as follows: 1 represents 0 to 2 mph, 2 represents 2 to 4 mph, 3 represents 4 to 6 mph.
2. "Time of Day" was created so tests were done under a variety of weather conditions.

Human PIR Detection Range = 33.8 + (1.42 x Sensor Elevation) – (0.0828 x Temperature)

S = 2.62670 R^2 = 83.1% Adjusted R^2 = 80.7%

PIR MAXIMUM VEHICULAR DETECTION RANGE

Detection Distance (Feet)	Sensor Elevation (Inches)	Cross Section[1]	Speed (MPH)	Time of Day[2]	Temperature (F)	Pressure (inHg)	Humidity (%)
150.6	12	3	19	6	64.9	30.15	53.3
86.2	3	3	8	9	75.1	29.76	70.6
79.2	5	1	11	4	70.6	30.15	33.4
110.8	8	2	13	16	77	29.97	94.9
124.1	11	2	39	2	59.3	30.2	51.4
93.8	4	2	50	13	57.4	30.00	94.1
109.0	2	3	33	5	54.5	30.12	82.8
143.6	11	3	30	15	100.7	29.6	23.9
104.0	6	2	28	8	88	29.80	77.2
72.1	0	1	36	10	64.9	30.15	53.3
86.4	9	1	47	7	106.8	29.57	20.3
100.5	7	3	44	12	41.8	29.62	95.1
101.4	5	2	42	0	36.4	28.68	93.6
80.6	1	2	16	14	93.6	29.74	46.7
102.4	8	2	5	3	81.4	29.88	84.2
73.7	10	1	22	11	57.6	29.56	85.5
60.3	2	2	25	1	61.5	29.85	83.6

Note:

3. Cross Section values are categorical. 1 represents a small car, 2 represents a small truck, 3 represents a large truck.
4. "Time of Day" was created so tests were done under a variety of weather conditions.

Vehicle Detection Range = 37.7 + (3.94 x Sensor Elevation) + (18.0 x Cross Section).

S = 13.0690 R^2 = 74.8% Adjusted R^2 = 71.3%

MAGNETOMETER MAXIMUM VEHICULAR DETECTION RANGE

Detection Distance (Feet)	Sensor Elevation (Inches)	Cross Section[1]	Speed (MPH)	Time of Day[2]	Temperature (F)	Pressure (inHg)	Humidity (%)
58.9	12	3	19	6	64.9	30.15	53.3
52.4	3	3	8	9	75.1	29.76	70.6
31.2	5	1	11	4	70.6	30.15	33.4
43.9	8	2	13	16	77	29.97	94.9
45.3	11	2	39	2	59.3	30.2	51.4
42.7	4	2	50	13	57.4	30.00	94.1
51.7	2	3	33	5	54.5	30.12	82.8
58.2	11	3	30	15	100.7	29.6	23.9
43.2	6	2	28	8	88	29.80	77.2
31.9	0	1	36	10	64.9	30.15	53.3
31.9	9	1	47	7	106.8	29.57	20.3
56.1	7	3	44	12	41.8	29.62	95.1
42.9	5	2	42	0	36.4	28.68	93.6
41.0	1	2	16	14	93.6	29.74	46.7
43.4	8	2	5	3	81.4	29.88	84.2
32.4	10	1	22	11	57.6	29.56	85.5
41.9	2	2	25	1	61.5	29.85	83.6

Note:

1. Cross Section values are categorical. 1 represents a small car, 2 represents a small truck, 3 represents a large truck.
2. "Time of Day" was created so tests were done under a variety of weather conditions.

Magnetic Detection Range = 17.6 + (0.415 x Sensor Elevation)+ (11.6 x Cross Section).

$S = 1.14515$ $R^2 = 98.6\%$ Adjusted $R^2 = 98.4\%$

PROBABILITY OF DETECTION AT 10 FEET

Detections	Missed Detections	Sensor Elevation	Cross Section	Speed	Time of Day	Temperature	Pressure	Humidity	Probability
100	0	12	3	19	6	72.1	29.89	30	1
99	1	3	3	8	9	64.3	29.86	39.8	0.99
98	2	5	1	11	4	81.6	29.82	56	0.98
100	0	8	2	13	16	67.8	30.03	84.5	1
100	0	11	2	39	2	91.2	29.77	66.9	1
99	1	4	2	50	13	52.9	30.15	82.1	0.99
100	0	2	3	33	5	69.9	30.01	67.4	1
100	0	11	3	30	15	64.6	29.9	41	1
99	1	6	2	28	8	87.7	29.77	50.1	0.99
98	2	0	1	36	10	57.6	29.85	83.6	0.98
98	2	9	1	47	7	100.7	29.6	25.3	0.98
100	0	7	3	44	12	64.9	30.15	53.3	1
100	0	5	2	42	0	102.2	29.73	20.4	1
99	1	1	2	16	14	41.8	29.62	94.3	0.99
99	1	8	2	5	3	38.2	28.67	92.7	0.99
99	1	10	1	22	11	54.5	30.12	82.6	0.99
99	1	2	2	25	1	77	29.96	33.6	0.99

$$P_{d\ 10\ Feet} = 0.974 + (0.000615 \times \text{Sensor Elevation}) + (0.00723 \times \text{Cross Section})$$

S = 0.00469833 R^2 = 65.9% Adjusted R^2 = 61.0%

PROBABILITY OF DETECTION AT 15 FEET

Detections	Missed Detections	Sensor Elevation	Cross Section	Speed	Time of Day	Temperature	Pressure	Humidity	Probability
100	0	12	3	19	6	72.1	29.89	30	1
99	1	3	3	8	9	64.3	29.86	39.8	0.99
98	2	5	1	11	4	81.6	29.82	56	0.98
100	0	8	2	13	16	67.8	30.03	84.5	1
100	0	11	2	39	2	91.2	29.77	66.9	1
99	1	4	2	50	13	54	30.14	76.2	0.99
100	0	2	3	33	5	76.3	29.97	71.6	1
100	0	11	3	30	15	67.8	30.03	84.5	1
99	1	6	2	28	8	91.2	29.77	66.9	0.99
97	3	0	1	36	10	57.6	29.85	83.6	0.97
98	2	9	1	47	7	100.7	29.6	25.3	0.98
100	1	7	3	44	12	64.9	30.15	53.3	1
100	0	5	2	42	0	102.2	29.73	20.4	1
99	1	1	2	16	14	41.8	29.62	94.3	0.99
99	1	8	2	5	3	38.2	28.67	92.7	0.99
98	2	10	1	22	11	54.5	30.12	82.6	0.98
99	1	2	2	25	1	77	29.96	33.6	0.99

$$P_{d\ 15\ Feet} = 0.967 + (0.000663 \times \text{Sensor Elevation}) + (0.00957 \times \text{Cross Section})$$

$S = 0.00469833$ $R^2 = 65.9\%$ Adjusted $R^2 = 61.0\%$

PROBABILITY OF DETECTION AT 20 FEET

Detections	Missed Detections	Sensor Elevation	Cross Section	Speed	Time of Day	Temperature	Pressure	Humidity	Probability
100	0	12	3	19	6	72.1	29.89	30	1
97	3	3	3	8	9	64.3	29.86	39.8	0.97
98	2	5	1	11	4	81.6	29.82	56	0.98
100	0	8	2	13	16	67.8	30.03	84.5	1
100	0	11	2	39	2	91.2	29.77	66.9	1
99	1	4	2	50	13	54	30.14	76.2	0.99
100	0	2	3	33	5	76.3	29.97	71.6	1
100	0	11	3	30	15	67.8	30.03	84.5	1
99	1	6	2	28	8	91.2	29.77	66.9	0.99
96	4	0	1	36	10	57.6	29.85	83.6	0.96
98	2	9	1	47	7	100.7	29.6	25.3	0.98
100	0	7	3	44	12	64.9	30.15	53.3	1
100	0	5	2	42	0	102.2	29.73	20.4	1
99	1	1	2	16	14	41.8	29.62	94.3	0.99
99	1	8	2	5	3	38.2	28.67	92.7	0.99
99	1	10	1	22	11	54.5	30.12	82.6	0.99
99	1	2	2	25	1	77	29.96	33.6	0.99

$$P_{d\ 20\ Feet} = 0.967 + (0.00143 \times \text{Sensor Elevation}) + (0.00705 \times \text{Cross Section})$$

$S = 0.00531346$ $R^2 = 71.3\%$ Adjusted $R^2 = 67.2\%$

PROBABILITY OF DETECTION AT 30 FEET

Detections	Missed Detections	Sensor Elevation	Cross Section	Speed	Time of Day	Temperature	Pressure	Humidity	Probability
100	0	12	3	19	6	70.6	30.15	33.4	1
97	3	3	3	8	9	77	29.97	94.9	0.97
98	2	5	1	11	4	59.3	30.2	51.4	0.98
100	0	8	2	13	16	67.8	30.03	84.5	1
99	1	11	2	39	2	91.2	29.77	66.9	0.99
99	1	4	2	50	13	54	30.14	76.2	0.99
99	1	2	3	33	5	76.3	29.97	71.6	0.99
100	0	11	3	30	15	100.7	29.6	23.9	1
99	1	6	2	28	8	88	29.8	77.2	0.99
96	4	0	1	36	10	64.9	30.15	53.3	0.96
98	2	9	1	47	7	93.6	29.74	46.7	0.98
100	1	7	3	44	12	64.9	30.15	53.3	1
100	0	5	2	42	0	102.2	29.73	20.4	1
99	1	1	2	16	14	41.8	29.62	94.3	0.99
99	1	8	2	5	3	38.2	28.67	92.7	0.99
99	1	10	1	22	11	54.5	30.12	82.6	0.99
97	3	2	2	25	1	77	29.96	33.6	0.97

$$P_{d\ 30\ Feet} = 0.964 + (0.00178 \times \text{Sensor Elevation}) + (0.0060 \times \text{Cross Section})$$

$S = 0.00909440$ $R^2 = 49.8\%$ Adjusted $R^2 = 42.6\%$

PROBABILITY OF DETECTION AT 40 FEET

Detections	Missed Detections	Sensor Elevation	Cross Section	Speed	Time of Day	Temperature	Pressure	Humidity	Probability
98	2	12	3	19	6	36.4	29.97	93.6	0.98
98	2	3	3	8	9	36.4	30.2	93.6	0.98
95	5	5	1	11	4	90.3	29.76	46.6	0.95
99	1	8	2	13	16	81.6	29.77	43.7	0.99
99	1	11	2	39	2	64.6	29.9	41	0.99
98	2	4	2	50	13	100.7	29.6	23.9	0.98
99	1	2	3	33	5	76.3	29.97	71.6	0.99
97	3	11	3	30	15	100.7	29.6	23.9	0.97
99	1	6	2	28	8	88	29.8	77.2	0.99
96	4	0	1	36	10	64.9	30.15	53.3	0.96
98	2	9	1	47	7	93.6	29.74	46.7	0.98
98	2	7	3	44	12	64.9	30.15	53.3	0.98
97	3	5	2	42	0	102.2	29.73	20.4	0.97
96	4	1	2	16	14	41.8	29.62	94.3	0.96
99	1	8	2	5	3	38.2	28.67	92.7	0.99
98	2	10	1	22	11	57.6	29.56	85.5	0.98
97	3	2	2	25	1	61.5	29.85	83.6	0.97

$$P_{d\ 40\ Feet} = 0.959 + (0.00123 \times \text{Sensor Elevation}) + (0.00525 \times \text{Cross Section})$$

S = 0.0110152 R^2 = 27.8% Adjusted R^2 = 17.5%

PROBABILITY OF DETECTION AT 50 FEET

Detections	Missed Detections	Sensor Elevation	Cross Section	Speed	Time of Day	Temperature	Pressure	Humidity	Probability
96	4	12	3	19	6	100.7	29.6	23.9	0.96
94	6	3	3	8	9	36.4	28.68	48.2	0.94
94	6	5	1	11	4	54.5	30.12	82.8	0.94
95	5	8	2	13	16	77	29.97	94.9	0.95
95	5	11	2	39	2	64.6	29.9	41	0.95
94	6	4	2	50	13	56.9	30.15	86.1	0.94
93	7	2	3	33	5	76.3	29.97	71.6	0.93
96	4	11	3	30	15	88	29.8	77.2	0.96
96	4	6	2	28	8	88	29.8	77.2	0.96
91	9	0	1	36	10	96.4	28.68	45.7	0.91
94	6	9	1	47	7	82.1	28.68	85.6	0.94
95	5	7	3	44	12	56.9	30.15	86.1	0.95
92	8	5	2	42	0	102.2	29.73	20.4	0.92
92	8	1	2	16	14	41.8	29.62	94.3	0.92
94	6	8	2	5	3	38.2	28.67	92.7	0.94
92	8	10	1	22	11	57.6	29.56	85.5	0.92
94	6	2	2	25	1	61.5	29.85	83.6	0.94

$$P_{d\ 50\ Feet} = 0.907 + (0.002277 \times Sensor\ Elevation) + (0.00889 \times Cross\ Section)$$

S = 0.0107493 R^2 = 50.2% Adjusted R^2 = 43.1.0%

PROBABILITY OF DETECTION AT 60 FEET

Detections	Missed Detections	Sensor Elevation	Cross Section	Speed	Time of Day	Temperature	Pressure	Humidity	Probability
95	5	12	3	19	6	56.9	30.15	86.1	0.95
94	6	3	3	8	9	102.2	29.73	20.4	0.94
94	6	5	1	11	4	54.5	30.12	82.8	0.94
95	5	8	2	13	16	77	29.97	94.9	0.95
95	5	11	2	39	2	64.6	29.9	41	0.95
93	6	4	2	50	13	100.7	29.6	23.9	0.93
93	7	2	3	33	5	36.4	28.68	48.2	0.93
96	4	11	3	30	15	88	29.8	77.2	0.96
96	4	6	2	28	8	61.5	29.85	83.6	0.96
91	9	0	1	36	10	96.4	28.68	45.7	0.91
93	7	9	1	47	7	82.1	28.68	85.6	0.93
95	5	7	3	44	12	56.9	30.15	86.1	0.95
92	8	5	2	42	0	76.3	29.97	71.6	0.92
93	7	1	2	16	14	41.8	29.62	94.3	0.93
94	6	8	2	5	3	38.2	28.67	92.7	0.94
92	8	10	1	22	11	57.6	29.56	85.5	0.92
94	6	2	2	25	1	57.4	30	94.1	0.94

$$P_{d\ 60\ Feet} = 0.908 + (0.00175 \times \text{Sensor Elevation}) + (0.00931 \times \text{Cross Section})$$

S = 0.0107493 R^2 = 50.2% Adjusted R^2 = 43.1%

PROBABILITY OF DETECTION AT 70 FEET

Detections	Missed Detections	Sensor Elevation	Cross Section	Speed	Time of Day	Temperature	Pressure	Humidity	Probability
95	5	12	3	19	6	104.3	29.57	22.6	0.95
93	7	3	3	8	9	45.6	29.77	91.8	0.93
93	7	5	1	11	4	34.9	29.74	93.4	0.93
92	8	8	2	13	16	96.4	28.68	45.7	0.92
93	7	11	2	39	2	88	30.12	23.9	0.93
93	6	4	2	50	13	59.3	29.74	77.2	0.93
91	9	2	3	33	5	62.4	29.88	76.2	0.91
95	5	11	3	30	15	88	29.8	77.2	0.95
96	4	6	2	28	8	61.5	29.85	83.6	0.96
88	12	0	1	36	10	96.4	28.68	45.7	0.88
93	7	9	1	47	7	34.9	28.68	93.4	0.93
94	6	7	3	44	12	96.4	29.74	45.7	0.94
91	9	5	2	42	0	82.1	29.88	85.6	0.91
93	7	1	2	16	14	88.2	29.8	75.7	0.93
92	8	8	2	5	3	38.2	28.67	92.7	0.92
91	9	10	1	22	11	57.6	29.56	85.5	0.91
93	7	2	2	25	1	57.4	30	94.1	0.93

$$P_{d\ 70\ Feet} = 0.893 + (0.00204 \times \text{Sensor Elevation}) + (0.0104 \times \text{Cross Section})$$

S = 0.00469833 R^2 = 65.9% Adjusted R^2 = 61.0%

PROBABILITY OF DETECTION AT 80 FEET

Detections	Missed Detections	Sensor Elevation	Cross Section	Speed	Time of Day	Temperature	Pressure	Humidity	Probability
94	6	12	3	19	6	104.3	29.57	22.6	0.95
93	7	3	3	8	9	45.6	29.77	91.8	0.93
93	7	5	1	11	4	34.9	29.74	93.4	0.93
92	8	8	2	13	16	96.4	28.68	45.7	0.92
93	7	11	2	39	2	88	30.12	23.9	0.93
93	6	4	2	50	13	59.3	29.74	77.2	0.93
91	9	2	3	33	5	62.4	29.88	76.2	0.91
94	6	11	3	30	15	88	29.8	77.2	0.95
93	7	6	2	28	8	61.5	29.85	83.6	0.96
87	13	0	1	36	10	96.4	28.68	45.7	0.88
93	7	9	1	47	7	34.9	28.68	93.4	0.93
94	6	7	3	44	12	96.4	29.74	45.7	0.94
91	9	5	2	42	0	82.1	29.88	85.6	0.91
93	7	1	2	16	14	88.2	29.8	75.7	0.93
92	8	8	2	5	3	38.2	28.67	92.7	0.92
91	9	10	1	22	11	57.6	29.56	85.5	0.91
90	10	2	2	25	1	57.4	30	94.1	0.93

$$P_{d\ 80\ Feet} = 0.893 + (0.00204 \times \text{Sensor Elevation}) + (0.0104 \times \text{Cross Section})$$

S = 0.0156504 R^2 = 38.2% Adjusted R^2 = 29.4%

MOTE-TO-MOTE BREAK RANGE

Distance	Elevation	Temperature	Pressure	Humidity
75.8	0	54	30.14	76.2
76.2	0	76.3	29.97	71.6
73.8	0	67.8	30.03	84.5
79.5	0	91.2	29.77	66.9
76.75	0	52.9	30.15	82.1
80.3	0	69.9	30.01	67.4
79.25	0	64.1	30	75.8
81.5	0	87.7	29.77	50.1
70.6	0	106.8	29.74	95.1
71	0	36.4	28.68	93.6
72.25	0	36.4	28.68	93.6
75.8	0	90.3	29.75	46.6
76.5	0	81.6	29.79	43.7
77.25	0	64.6	29.9	41
71.2	0	100.7	29.6	23.9
67.1	0	36.4	28.68	48.2
100.2	6	63.9	30.15	53.1
95.4	6	72.7	29.76	71.3
99.5	6	71.6	30.15	33.4
105.4	6	75.4	29.97	90.4
101.3	6	61.2	30.2	53.7
93.25	6	59.7	30	92.1
94.75	6	51.1	30.12	85.3
102.25	6	102.8	29.6	20.4
98.5	6	88.2	29.8	75.7
99.66	6	62.4	30.15	53.3
93.5	6	104.3	29.57	22.6
102.5	6	45.6	29.62	91.8
100.25	6	34.9	28.68	93.4
103.1	6	96.4	29.74	45.7
94.22	6	82.1	29.88	85.6
96.22	6	56.9	29.56	86.1
136.75	12	64.9	30.15	53.3
140.8	12	75.1	29.76	70.6
122.75	12	70.6	30.15	33.4
145.8	12	77	29.97	94.9
125.4	12	59.3	30.2	51.4
138.75	12	57.4	30	94.1
140.25	12	54.5	30.12	82.8
136.43	12	100.7	29.6	23.9
125.8	12	88	29.8	77.2
144.5	12	59.3	30.2	51.4
138.9	12	57.4	30	94.1
130.6	12	54.5	30.12	82.8
139.66	12	100.7	29.6	23.9
150.22	12	88	29.8	77.2
141.66	12	64.9	30.15	53.3
143.33	12	106.8	29.57	20.3

MOTE-TO-BASE STATION BREAK RANGE

Distance	Elevation	Temperature	Pressure	Humidity
51.8	0	54	30.14	76.2
53.75	0	76.3	29.97	71.6
50.75	0	67.8	30.03	84.5
56.2	0	91.2	29.77	66.9
49.1	0	52.9	30.15	82.1
51.8	0	69.9	30.01	67.4
55.1	0	64.1	30	75.8
53.6	0	87.7	29.77	50.1
46.9	0	106.8	29.74	95.1
47.8	0	36.4	28.68	93.6
54.8	0	90.3	29.75	46.6
55.9	0	81.6	29.79	43.7
53.1	0	64.6	29.9	41
54.9	0	100.7	29.6	23.9
50.9	0	36.4	28.68	48.2
47.2	0	54.5	30.12	82.8
80.7	6	77	29.97	94.9
90.5	6	59.3	30.2	51.4
82.1	6	57.4	30	94.1
88.7	6	54.5	30.12	82.8
93.2	6	100.7	29.6	23.9
91.9	6	88	29.8	77.2
91.7	6	64.9	30.15	53.3
90.3	6	93.6	29.74	46.7
89.5	6	81.4	29.88	84.2
89.5	6	75.1	29.76	70.6
90.9	6	70.6	30.15	33.4
81.4	6	77	29.97	94.9
93.8	6	59.3	30.2	51.4
84.3	6	57.4	30	94.1
93.9	6	54.5	30.12	82.8
94.8	6	100.7	29.6	23.9
115.5	12	88	29.8	77.2
120.3	12	57.6	29.56	85.5
119.7	12	61.5	29.85	83.6
120.3	12	63.9	30.15	53.1
114.9	12	72.7	29.76	71.3
117.8	12	71.6	30.15	33.4
112.8	12	34.9	28.68	93.4
118.3	12	96.4	29.74	45.7
113.5	12	82.1	29.88	85.6
114.8	12	88.2	29.8	75.7
118.66	12	62.4	30.15	53.3
120.33	12	104.3	29.57	22.6
110.4	12	34.9	28.68	93.4
116.7	12	96.4	29.74	45.7
114.01	12	64.3	29.86	39.8
104	12	81.6	29.82	56

MOTE-TO-MOTE REASSOCIATION RANGE

Distance	Elevation	Temperature	Pressure	Humidity
36.2	0	54	30.12	85.3
38.25	0	76.3	29.6	20.4
39.5	0	67.8	29.8	75.7
40.2	0	51.1	30.15	66.9
38.8	0	102.8	29.97	82.1
40.7	0	88.2	30.01	67.4
39.4	0	59.7	30	75.8
40.1	0	91.2	29.76	50.1
34.9	0	106.8	30.15	95.1
35.4	0	36.4	29.97	93.6
26.9	0	36.4	30.2	93.6
39.5	0	90.3	29.76	46.6
38.8	0	81.6	29.77	43.7
39.1	0	64.6	29.9	41
35.4	0	100.7	29.6	23.9
36.85	0	36.4	28.68	48.2
49.5	6	63.9	30.15	53.1
50.25	6	72.7	29.75	71.3
51.75	6	71.6	29.79	33.4
42.8	6	75.4	30.15	90.4
48.1	6	61.2	30.2	53.7
43.1	6	100.7	30	92.1
47.3	6	88	30.12	23.9
48.2	6	59.3	29.74	77.2
47.6	6	62.4	29.88	76.2
46.9	6	54.5	29.56	53.3
47.1	6	104.3	29.57	22.6
44.9	6	45.6	29.77	91.8
45.9	6	34.9	29.74	93.4
46.2	6	96.4	28.68	45.7
46.8	6	82.1	28.68	85.6
47.2	6	56.9	30.15	86.1
55.9	12	64.9	30.15	53.3
54.7	12	75.1	29.62	70.6
57.75	12	70.6	28.68	33.4
50.25	12	77	29.6	94.9
54.3	12	59.3	29.8	51.4
51.7	12	57.4	30	94.1
52.9	12	54.5	30.14	82.8
55.8	12	57.4	29.97	51.4
52.1	12	87.7	30.03	94.1
55.2	12	52.9	30.2	82.8
54.8	12	69.9	30	71.6
53.9	12	64.1	30.12	84.5
56.3	12	100.7	29.6	23.9
57.1	12	88	29.8	77.2
57.2	12	64.9	30.15	53.3

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. HEAT REMOVAL CONCERNS

A. OVERVIEW

The use of digital video surveillance imagery in tactical networking environments provides the watch-stander with significantly increased intelligence, surveillance, and reconnaissance capabilities. The role of the cameras in the integrated network is to provide remote, real-time visual information to a watch-stander. This offers several key benefits, including visual verification of sensor activity, remote monitoring, and persistent surveillance. Providing real-time visual information assists decision makers in making accurate and timely decisions. However, most commercially available internet protocol (IP) cameras are not designed to function in the harsh environments commonly found in military and law enforcement applications. As a result of several field exercises and feedback from coalition military forces and in conjunction with Kestrel Technology Group, several design modifications have proposed to commercially available IP cameras to increase the longevity and reliability of digital surveillance equipment in high temperature environments. Additionally, the principles used during this research are applicable to other electronics used in field operations.

B. INTRODUCTION TO AXIS 213 PTZ NETWORK CAMERA

Numerous law enforcement and military organizations currently use video surveillance technologies on a daily basis. As a result, numerous commercial companies have begun developing video products designed for remote monitoring and security applications. Among the most prolific of such companies is Axis Communications, which is a global market leader in network video products and specializes in "professional network video solutions for remote monitoring, security surveillance and broadcasting (www.axis.com/corporate/index.htm)."

The Axis 213 PTZ Network Camera, shown in Figure 1, is the video component selected for use. The camera was selected for several important reasons. Firstly, the Axis 213 camera is currently in use by several military and law enforcement organizations worldwide. It is currently in use by several United States military organizations such as the Air Force Force Protection Battle Lab. Additionally, the Axis

213 is currently used by the Royal Thai Military Forces operations in support of the Global War on Terror. Secondly, the size and shape of the Axis 213 is conducive for covert operations and concealment. Additionally, the camera does not consume significant amounts of power and can easily be powered for extended time periods on a common car battery. Finally, the Axis 213 is an easily available commercial camera package that provides significant performance capabilities in a single, cost-efficient package. The camera offers impressive pan, tilt, and zoom functions combined with built-in infrared capabilities, adjustable frame rates, multiple video stream formats, and preset viewing positions. Table 1 provides details of the important performance capabilities of the Axis 213 PTZ Network Camera.

Figure 1 Axis 213 PTZ Network Camera

Capability	Specification
Lens	2.5 – 91mm F1.6 –F4.0, motorized zoom lens Horizontal viewing angle: 42 – 1.7º Auto focus, 26x optical and 12x digital zoom
Minimum Illumination	Color mode: 1 lux, F1.6 IR mode: 0.1 lux, F1.6* *Using built in IR light in complete darkness up to 3 meters
Video Compression	Motion JPEG MPEG-4
Resolutions	704x480, 768x576, 160x120, 176x144
Frame Rates	Motion JPEG: Up to 30/25 frames per second MPEG-4: 30/25 or 21/17 frames per second
Video Streaming	Simultaneous Motion JPEG and MPEG-4 Controllable frame rate and bandwidth Constant and variable bit rate
Pan Angle Range	340º
Tilt Angle Range	100º
Zoom	26x optical, 12x digital
Preset Positions	20 operator definable preset positions and configurable monitoring sequence
Video Access	Up to 20 simultaneous clients
Supported Protocols	IP, HTTP, TCP, ICMP, RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, UpnP, ARP, DNS, DynDNS, SOCKS
Connectors	RJ-45 26-pin multi-connector
Power	13 V DC, max 24 W external power supply
Operating Conditions	5 – 40 ºC (41 – 104 ºF) 20 – 80 % non-condensing relative humidity
Dimensions (HxWxD) and Weight	130 x 104 x 130 mm (5.12 x 4.09 x 5.12 in) 700 grams (1.55 pounds)

Table 1 Axis 213 Capabilities from Axis User's Manual (Axis, 2005)

C. THE PROBLEM

The Axis 213 camera is a surveillance package designed primarily for indoor use in moderate climactic environments. The maximum temperature of 104 ºF makes the unmodified camera inappropriate for most military and law enforcement applications. For example, during the Coalition Operating Areas Surveillance and Targeting System (COASTS) March demonstrations in Chiang Mai, Thailand, the Axis 213 suffered from many heat related performance problems. During the demonstrations, the ambient temperature would routinely exceed 104 ºF. The camera would continue to function until

the base of the camera reached almost 106 ºF. Once the temperature of the camera peaked, the camera would overheat and stop functioning. The camera became unreachable via the 802.11 network or by direct Ethernet connection. It was suspected that the microchips associated with the web server were overheating. When the camera overheated, the power lights would remain lit, but the camera would not respond to network pings, nor would it be accessible through a web browser. Upon failure, the camera was placed in the shade and allowed to cool. Once it cooled, the camera began operating correctly until it overheated. On days when the ambient temperature was under 100 ºF, the camera operated correctly without failure.

The performance problems are indicative solely of overheating. Typically, when electronics suffer from heat problems, a specific chip (or set of chips) will fail and affects specific functions until sufficiently cooled. This was verified through contacting the Axis technical support. They confirmed that the chips associated with the web server are typically the first chips to overheat. Failure was repeated several times in the laboratory by placing the camera inside of an oven. The symptoms seen in the lab were consistent with those found in Thailand and described by the Axis technical support staff.

As a result of the COASTS demonstrations and feedback from Thai security forces currently using the Axis 213 camera, and in conjunction with contractors from Kestrel Technology Group, several design modifications have been undertaken to increase the longevity and reliability of the Axis 213 in high temperature environments. The primary goals of the modifications are to improve heat extraction from electronic components while simultaneously minimizing environmental heat intake to the camera and ensuring full range of Pan-Tilt-Zoom capabilities.

D. COOLING METHODS

Several heat reduction and removal approaches exist for hardening electronic equipment operating near or above the maximum rated environmental temperature. After analyzing the Axis 213, two cooling methods have been developed: the controlled housing temperature approach and the chip cooling method. The following sections discuss the two methods in detail.

1. Controlled Housing Temperature Approach

The first, and most challenging, approach to removing heat at ambient temperatures at or above the rated temperature is the controlled housing temperature approach. This approach entails employing active and passive techniques to regulate the external camera housing at a temperature below the maximum operating temperature. The controlled housing temperature approach uses a solid state thermoelectric cooler and heat sink combination to cool the housing and associated electronics to a temperature below the ambient environmental temperature. This approach is the most robust approach because the entire electronic system is kept at a nearly constant temperature regardless of the surrounding environment. The controlled temperature approach, however, is more expensive and requires larger heatsinks and results in greater power consumption. As a result, the approach is recommended for fixed locations where power is easily available as opposed to applications with strict size and weight constraints. Using the controlled housing temperature approach is expected to maximize the effective component life through maintaining a steady temperature without the use of any moving parts. As a result, this method is expected to be most suitable for operations in extreme environments such as Thailand, Afghanistan, and Iraq.

The controlled housing temperature approach consists of two major components. The first component is a solid state thermoelectric cooler. Peltier devices are common thermoelectric coolers used for electronic applications. A Peltier device, shown in Figure 2, is typically a few centimeters square and only a few millimeters deep. They consist of small Bismuth Telluride cubes that behave as a heat pump (Thermoelectric Handbook, 2006). Heat is moved from one side of the device to the other by applying a current source. The "cold" side of the device is typically applied to devices such as microprocessors and other sensitive electronic equipment. The "hot" side of the device reaches high temperatures and is commonly attached to a heatsink for heat removal ("Thermoelectric Cooler FAQ," 2006). A thermostatic control switch can be added to activate the Peltier device only when a specified temperature is achieved. The combination of a Peltier device and a control switch allows the system to behave much like the thermostat for an air conditioning system. When the temperature of the device on

the “cold” side of the Peltier cooler is higher than the specified temperature, the Peltier cooler is activated and runs until the device is below the temperature threshold.

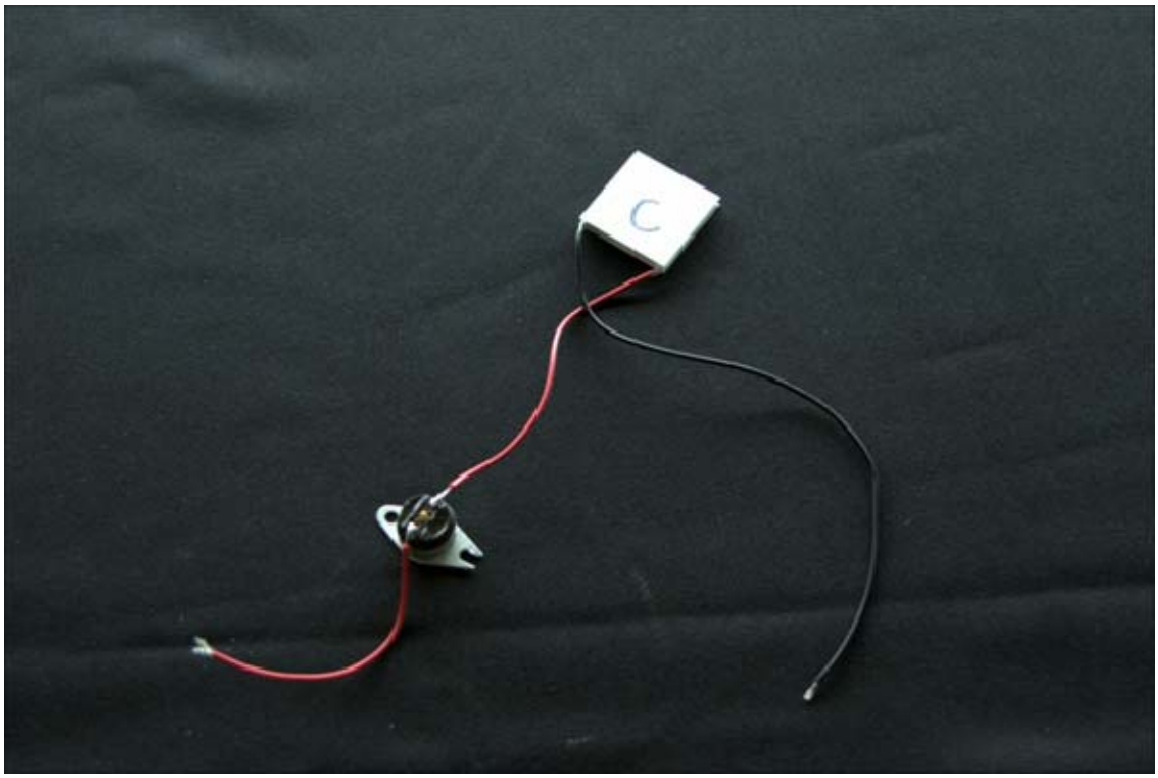


Figure 2 Peltier Cooler with Temperature Control Switch

The second component of the controlled housing temperature method is a heatsink. There are two types of heatsinks available. The first heatsink type is the passive heatsink. Passive heatsinks consist of a thermally conductive metal with at least one flat side which is attached to the object being cooled and an arrangement of fin-like protrusions. The flat part of the heat sink must maintain good thermal contact with the object. Traditionally, thermal grease or gap filler is applied to ensure smooth and continuous contact. The fins of the heat sink are used to increase the surface contact with the surrounding air. Passive heatsinks are typically composed of either copper or aluminum due to their excellent thermal conducting properties. Copper heatsinks are more expensive but are also more efficient thermal conductors. Figure 3 shows a common passive heatsink. The active heatsink is the second type of common heatsink. Active heatsinks use fans in conjunction with a passive heatsink to remove excess heat

from an object. The fan increases the airflow over the heatsink, thus maintaining a larger temperature gradient. By creating a larger temperature gradient, the heat sink can remove heat more quickly and also can operate in slightly higher ambient temperatures (Heatsink ABCs, 2006). However, adding a fan also creates the possibility of equipment failure due to the moving parts. Figure 4 shows a typical active heatsink.

Figure 3 Passive Heatsink

Figure 4 Active Heatsink

2. Chip Cooling Method

The second cooling approach is the chip cooling method. The chip cooling method involves removing heat from the hottest components on a circuit board. The chip cooling method is commonly used by manufacturers that identify specific chips as being at risk of overheating. Typically the identified chips operate several degrees hotter than the ambient temperature and the other surrounding circuitry. The chip cooling method involves spreading the heat generated by the chips more evenly across other components and the surrounding air. Two chip cooling methods exist. The first method is heat spreading. Heat spreading uses thin thermal metals which attach to the chip. The heat spreader, shown in Figure 5, disperses the heat over a large area and increases heat removal by adding more surface area. The second method involves increasing the airflow over hot chips. If the air temperature is lower than the chip's temperature, heat will be removed from the chip. Although the fan adds a possible point of failure, internally mounted fans are typically suitable for cooling applications. The chip cooling methods are often used in conjunction with thermal grease or thermal gap filler. The grease and gap filler serve to efficiently transfer the heat generated by the chips to other sources such as the external casing. The two approaches can easily be combined to create an efficient, low-cost solution for many heat reduction projects.

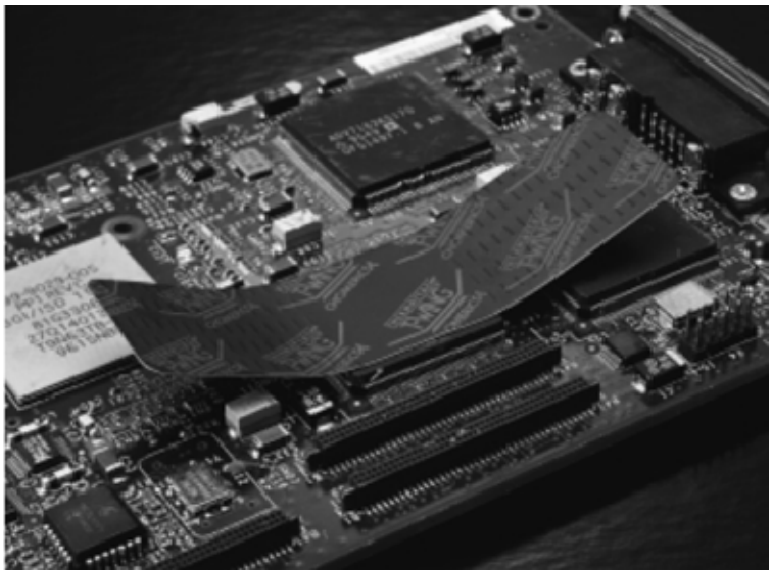


Figure 5 T-Wing Heat Spreader Attached to a Microchip (Chomerics T-Wing Data Sheet)

E. PROTOTYPED COOLING SOLUTION

Two prototyped cooling solutions for the Axis 213 camera have been designed. Both solutions involve a combination of the controlled housing temperature approach and the chip cooling approach. Both solutions have been designed, priced, and built. However, due to time constraints, only one method will be tested. After conducting experiments to determine the amount of excess heat needed to be removed, it was discovered that the Axis 213 need roughly 10 Watts of heat removal to ensure operation at temperatures in excess of 110 ºF. The following sections describe the two prototypes designed by Naval Postgraduate School students in conjunction with Kestrel Technology Group.

1. Active Heatsink with Chip Cooling Method

The first custom solution designed for the Axis 213 camera combined aspects of both the controlled housing temperature method and the chip cooling method. Upon opening the camera's case, three chips were identified as being candidates for overheating. Additionally, it was obvious that the manufacturer had identified the same chips. A substance similar to thermal gap filler was placed between the chips and a large metal plate which connected to the camera's base. However, the connection between the chips and the metal plate was not reliable. Additionally, the metal plate, which acts like a heat spreader, was not firmly connected to the base of the camera. It became apparent that the heat reduction design could be improved through ensuring solid connections between the existing materials. A thick layer of thermal grease was applied between the chips and the thermal gap filler material. Additionally, another layer of grease was applied between the metal plate and the base of the camera. Once solid connections were made and allowed to dry, the camera was reassembled. Next, an active heatsink was chosen to help extract heat from the camera's case. The heatsink chosen was the Thermaltake Extreme Volcano 12. The Thermaltake, shown in Figure 6, is designed to act as a processor cooler for computers. It consists of a high density copper core with 66 fins to increase surface area. Additionally, it has an 80mm x 80mm x 32mm three blade fan with ball bearings, which is capable of producing airflow of nearly 72.92 cubic feet

per minute (User's Manual, 2006). The Thermaltake active heatsink is a cost-effective solution that is able to remove over 70 Watts of heat with the fan at maximum speed. Finally, the Thermaltake heatsink has a life expectancy of 80,000 hours.

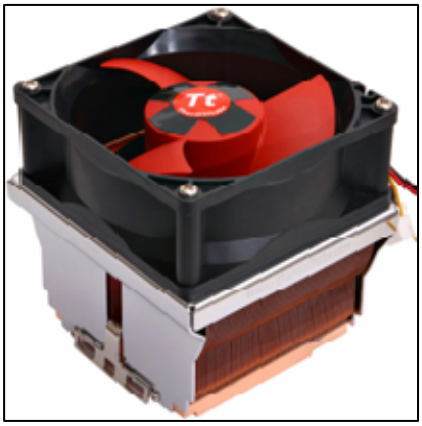


Figure 6 Thermaltake Extreme Volcano 12 Active Heatsink

The heatsink connected to the base of the camera using thermal gap filler in addition to thermal grease. The combination of thermal gap filler and thermal grease created a strong connection between the heatsink and the camera. A strong connection is beneficial for both heat removal and for ensuring the camera does not fall off of the heatsink while in the field. Figure 7 shows the modified Axis 213.

Figure 7 Modified Axis 213

2. Controlled Housing Temperature Method

The second heat removal modification focuses on the controlled housing temperature method. As discussed previously, the controlled housing temperature method is more expensive but has greater potential as a long term solution for deploying cameras in high temperature environments. The first step in this method was to re-seal the connection between the overheating chips and the base of the camera. This ensures the maximum amount of heat would be transferred to the base of the camera. Next, a Peltier device was soldiered to a temperature control switch. The control switch was set to 90 ºF. Once the object attached to the "cold" side of the Peltier device exceeded 90 ºF, the switch would activate the Peltier cooler until the object was below 90 ºF. The temperature threshold was chosen because 90 ºF is well under the maximum rated temperature of 104 ºF. Additionally, 90 ºF would be above the dew point found in most hot environments. As a result, no condensation would form and potentially harm the system. Finally, a heatsink was added to the "hot" side of the Peltier device. Both custom passive and conventional active heatsinks were considered. The passive design is preferred because it provides maximum reliability due to a lack of moving parts. However, custom passive heatsinks are often expensive. A single 7 x 7 inch passive heat sink costs roughly $150. In bulk, however, the price falls to roughly $45 per unit. The

Thermaltake heatsinks, on the other hand are easily available for under $35 dollars per unit. For the purposes of this research, the Thermaltake active heatsinks were used. Figure 8 shows the controlled housing temperature design prototype.

Figure 8 Controlled Housing Temperature Design Prototype

F. EXPERIMENTS AND DEMONSTRATIONS

Several experiments and demonstrations were created to test the effectiveness of the designs. Initially, a rudimentary heat chamber was created using a Styrofoam box and a heat lamp. The maximum temperature reached in this apparatus was 102 ºF. Although the maximum rated temperature of 104 ºF was not reached, the base of the camera was over 104 ºF. Next, an unmodified Axis 213 was placed inside of an oven. Temperature was crudely regulated through slightly opening the oven door to allow heat to escape. The unmodified version of the camera failed at an ambient temperature of 106 ºF. When the ambient temperature was 106 ºF, the temperature of the camera's base was only 104 ºF.

Having induced camera failure of an unmodified camera in a controlled method, the camera was incrementally modified. First, the only modifications made were the chip cooling modification. The overheating chips were sealed to the internal metal plate and the plate was sealed to the base of the camera. No heat sinks were added for the first iteration of testing. The modified camera was again placed in the oven. During this iteration, a noticeable increase was observed. When the ambient temperature reached

106 ºF, the base of the camera reached 108 ºF. This indicates increase heat removal efficiency. The Axis camera did not fail until the ambient temperature reached 112 ºF and the base temperature was 109 ºF. At this point, the camera was removed from the oven and allowed to cool to room temperature. Next, the Thermaltake Extreme Volcano heatsink was applied to the base of the Axis 213 using thermal gap filler and thermal grease. Once a firm seal was formed between the camera and the heatsink, the modified camera was again placed inside the oven without activating the heatsink's fan. The temperature was regulated at the previous maximum temperature of 112 ºF for 30 minutes. During this time, the camera maintained full functionality. There was no perceptible loss in optics (zoom or focus) capabilities, controllability (pan and tilt), or in connectivity. The temperature was increase to 125 ºF and regulated for another 30 minutes. Again, there was no perceptible impact on the camera. The temperature was then increased to 135 ºF and regulated for another 30 minutes. Even at that temperature, there was no significant loss of capabilities. Finally, the temperature was increase to 145 ºF for 30 more minutes. At this temperature the camera maintained full functionality, controllability, and connectivity. Temperature measurements were taken of the camera's base and the fins of the heat sink. The temperatures achieved equilibrium at 145 ºF. At this point, the tests were stopped for fear of causing irreparable damage to the camera.

As the initial tests indicated that a fully passive solution was sufficient for full operations in Thailand, no tests with the controlled housing temperature design were conducted. The active heatsink with chip cooling design was implemented on all but one of the ground-based cameras during the COASTS deployment of May, 2006. During the COASTS deployment, several field tests were conducted. The first field test conducted was a comparison between an unmodified Axis 213 and the modified version. The two cameras were placed in the same area. The cameras were roughly one foot apart to ensure they both had the same environmental exposure. The unmodified version of the camera failed at 103 ºF while the modified version maintained full functionality. At this point, the final camera was modified to the active heatsink with chip cooling design. On two occasions, the modified version of the camera suffered failures. There are two possible explanations for the failures. The first is that the effects of the heat were compounded by extremely high non-condensing humidity levels. During both failures,

the humidity was in excess of 95%. This value is higher than the rated 80% non-condensing humidity level. The second, and more probable, explanation is the ambient temperature was increased due to plastic jugs used to shield the cameras from rain. During both failures, the cameras were placed inside of opened water jugs to provide protection from fast moving rain showers. The temperature inside of the jugs was measured and determined to be over 112 ºF while the ambient temperature was only 107 ºF. Additionally, when the cameras were removed from the jugs they immediately began functioning correctly. A final comparison test was performed. One camera was placed inside of the jug with the Thermaltake heatsink's fan active while the other camera was place in a jug without the fan running. The camera without the fan failed at an ambient temperature of 108 ºF. At the point of failure, the temperature inside of the jug was 114 ºF. The camera with the active fan continued to function correctly with the temperature inside the jug at 115 ºF. At this point, it was decided that all ground cameras should use the fan assisted heatsinks to ensure operation during all demonstration and scenario exercises. Figure 9 shows the modified Axis cameras in use during the COASTS scenario demonstration.

Figure 9 Modified Axis Cameras as Deployed During the COASTS Scenario

G. CONCLUSIONS

1. Summary

This research focused on developing a cost-effective way to efficiently remove heat from commercially available digital video surveillance cameras. The Axis 213 network camera was analyzed based upon the needs of the COASTS program and feedback from coalition military forces currently using the camera in daily operations. During previous deployments, the Axis camera commonly suffered from heat related failure at or near the maximum rated temperature. However, the camera is currently used by military and law enforcement agencies in high temperature environments. Camera failures in these environments have risked the lives of the forces depending upon the camera for video surveillance. Common cooling approaches were discussed in detail. The heat reduction techniques discussed are also applicable to all electronic equipment used in field operations. Two heat removal prototypes have been developed for use with the Axis 213 camera. The active heatsink with chip cooling prototype was thoroughly

tested in laboratory experiments in Monterey, CA, and in field exercises during the COASTS deployment to Thailand. Unfortunately, the controlled housing temperature prototype was not tested due to time and money constraints.

2. Analysis

The COASTS Thailand demonstrations clearly showed the noticeable increase in performance due to the addition of heat removal modifications to the Axis 213 camera. The passive version of the tested modifications saw an 8% increase in the failure temperature while the active version did not fail at a 12% increase in the failure temperature. Although the fully passive version of the design did not perform as well in the Thailand demonstrations as it did in laboratory tests, a significant improvement over the unmodified camera was noticed. In active mode, the camera remained fully functional with the surrounding temperature reaching 115 ºF. It is expected that camera will continue to function in temperatures up to 125 ºF with the fan activated. Most military and law enforcement operations occur in temperatures under the 115 ºF mark. The average maximum temperature in Thailand is roughly 112 ºF, suggesting that the current design prototype would be sufficient for continued use (Thailand Weather Data, 2006).

The addition of heat removal solutions for digital surveillance cameras is highly recommended for military and law enforcement agencies. Most electronic equipment is not designed to operate harsh climactic environments. Heat and moisture are the two leading challenges facing the integration of commercial-off-the-shelf technologies into military applications. Heat related failures cause significant degradation of capabilities, increases the costs of operations, and puts operators' lives at risk. The tested heat removal design was built entirely from commercially available material for minimal cost. The entire modifications cost roughly $50. The design, though rudimentary, greatly increased the deployability of the Axis camera. The controlled housing temperature prototype can be built and implemented for roughly $200. Although the controlled housing temperature design costs more than the chip cooling design, it is significantly less than the cost of a new camera. Additionally, the controlled housing temperature approach offers the greatest potential due to the ability to regulate the temperature lower

than the maximum rated threshold. A steady temperature is expected to greatly benefit the life of the components as the stress from contraction and expansion due to heat does not occur. The minimal investment for heat reducing modifications can help significantly increase the lifespan of the camera, reduce replacement and maintenance costs, and protect operators and technicians in the field.

3. Avenues for Future Research

Several areas for future research have emerged. The most pressing avenue for research is the refinement and testing of the controlled temperature housing design. Because the design regulates the camera's temperature regardless of the ambient temperature, the experiments must be conducted in true heat chambers. Conducting the test in heat chambers will allow more precise control of the experiment. Additionally, tests can be conducted to determine the minimum size heatsink need to ensure the camera can function at temperatures in excess of 130 ºF. Creating the most space efficient design is beneficial for covert placement in military and law enforcement applications. Finally, research should be done to develop solar shields to protect the cameras from direct sun exposure. For example, heat rejecting materials can be used to create a "sun shield." However, it is important that no design modifications hinder the optical or controllability of the devices.

LIST OF REFERENCES

"Chomerics T-wing Data Sheet." Chomerics. Online. Last accessed: 7 JUNE 06.
<http://www.chomerics.com/products/twing.htm>

"Heatsink ABCs". Computerhope. Online. Last accessed: 6 JUNE 06
<http://www.computerhope.com/help/heat.htm>

"Thailand Weather Data." Online. Last accessed: 8 JJUNE 06
<http://www.ourweb.info/01/weather/>

"Thermoelectric Cooler FAQ." Tellurex. Online. Last accessed: 5 JUNE 06.
<http://www.ourweb.info/01/weather/>

"Thermoelectric Handbook." Melcor. Online. Last accessed: 8 JUNE 06. <http://www.melcor.com/pdf/Thermoelectric%20Handbook.pdf>

Thermaltake Extreme Volcano 12 User's Manual. Thermaltake. Online. Last accessed: 8 JUNE 06. < http://www.thermaltake.com/coolers/volcano/rs/a1745.htm>

LIST OF REFERENCES

"Design Methods Fact Sheet." University of Queensland. MECH4551 Class.

"Joint Vision 2020," US Government Printing Office, June 2000, Last Accessed 01/06. http://www.dtic.mil/jointvision/jvpub2.htm.

"Navy Concept Development and Experimentation Expeditionary Power Projection," June 2001, Last Accessed 01/06. http://www.dtic.mil/ndia/2001ewc/ncde.pdf.

"Test and Evaluation Planning Guide for Combating Terrorism and Public Safety Systems and Products." Technical Support Working Group. Last Accessed 01/06. http://www.tswg.gov/tswg/techtrans/tech_trans.htm.

Al-Karaki, J., Kamal, A. (2005). A Taxonomy of Routing Techniques in Wireless Sensor Networks. In Ilayas, M., Mahgoub, I.. (Eds.) Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems. Boca Raton.

Axis Communications. "About Axis." Last Accessed 05/06. www.axis.com/corporate/index.htm.

Bragnisky, D. and Estrin, D., "Rumor Routing Algorithms for Sensor Networks," Proceedings *of Association for Computer Machinery Workshop on Wireless Sensor Networks and Applications 2002*, pp. 22-31, September 2002.

Callaway, E., Jr., *Wireless Sensor Networks Architectures and Protocols*, pp. 21-44, Auerbach Publications, New York, 2004.

Clark, V., "Sea Power 21," *Proceedings*, October 2002, Last Accessed 12/05. http://www.chinfo.navy.mil/navpalib/cno/proceedings.html.

Compact Wireless and Wired Sensing Systems. Boca Raton.

Cottrell, Les, Matthews, Warren and Logg, Connie, Stanford Linear Accelerator Center, "Tutorial on Internet Monitoring & PingER at SLAC," Last Accessed 02/06. http://www.slac.stanford.edu/comp/net/wan-mon/tutorial.html.

Crossbow (2005). "Getting Started Guide." Last accessed 04/06. http://www.xbow.com/Support/Support_pdf_files/Getting_Started_Guide.pdf.

Crossbow (2005). Last Accessed 06/06. http://www.xbow.com.

Culler, D., Estin, D. and Strivastava, M. (2004, August) Overview of Sensor Networks. Computer, 37, 41-49.

Culler, D. and Hong, W. (Eds.) (2004, June). Wireless Sensor Networks. Communication of the ACM, 47, 30-33.

DACS, "A History of Software Measurement at Rome Laboratory," Last accessed 01/06. http://www.dacs.dtic.mil/techs/history/His.RL.2.2.html.

Elson, J. and Estrin, D., "Time Synchronization for Wireless Sensor Networks," *Proceedings of IEEE IPDPS Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing 2001*, pp. 1965-1970. April 2001.

Feibel, W. (1995). The Encyclopedia of Networking. Alameda.

Haenggi, M. (2005). *Opportunities and Challenges in Wireless Sensor Networks*. In Ilayas, M., Mahgoub, I.. (Eds) Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems. Boca Raton.

He, T., Stankovic, J. A., Lu, C. and Abdelzaher, T., "SPEED: A Stateless Protocol for Real-Time Communications in Sensor Networks," *Proceedings of IEEE International Conference on Distributed Computing Systems 2003*, pp. 46-57, May 2003.

Heinzelman, W., Chadrakasan, A. and Balakrishnan, H., "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," Proceedings of Hawaii International Conference on System Sciences 2000, pp. 4-7, January 2000.

Holger, K. And Willig A. (2005). Protocols and Architectures for Wireless Sensor Networks. London.

IEEE Std. 802.15.4 -2003, "IEEE Standard for Information Technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 15.4: Wireless Medium Access Control and Physical Layer Specifications for Wireless Personal Area Networks," Last accessed 12/05. http://standards.ieee.org/getieee802/802.15.html.

Lu, C., Blum, B. M., Abdelzaher, T. F., Stankovic, J. A. and He, T., "RAP: A Real-Time Communication in Sensor Networks," *Proceedings of IEEE Real Time and Embedded Technology and Applications Symposium 2002*, pp. 55-66, September, 2002.

Nasipuri, A. and Li, K., "A Directionality-Based Localization Scheme for Wireless Sensor Networks," Proceedings of Association for Computing Machinery Workshop on Wireless Sensor Networks and Applications 2002, pp. 105-111, September 2002.

Ofek, Y., "Generating a Fault-Tolerant Global Clock Using High-Speed Control Signals for the MetaNet Architecture," IEEE/ACM Transactions on Networking, vol. 3, pp. 1650-1654, 2002.

Pahlavan, K. and Krishnamurthy, P., *Principles of Wireless Sensor Networks*, pp 415-532, Prentice Hall, Upper Saddle River, New Jersey, 2004.

Perrig, A., Szewcyzk, R., Wen, V., Culler, D. E. and Tygar, J. D., "SPINS: Security Protocols for Sensor Networks," *Proceedings of Association for Computing Machinery Mobile Computing and Networking 2001*, pp. 189-199, July 2001.

Raghunathan, V., Schurgers, C., Park, S. and Srivastava, M., "Energy-Aware Wireless Microsensor Networks," IEEE Signal Processing Magazine, vol. 19, no. 2, pp. 40-50, March 2002.

Savvides, A., Han, C. and Srivastava, M. B., "Dynamic Fine-Grained Localization in Ad Hoc Networks of Sensors," *Proceedings of Association for Computing Machinery Mobile Computing and Networking 2001*, pp. 166-179, July 2001.

Shih, E., Cho, S., Ickes, N., Min, R., Sinha, A., Wang, A. and Chandrakasan, A., "Physical Layer Driven Protocol and Algorithm Design for Energy-Efficient Wireless Sensor Networks," *Proceedings of Association for Computer Machinery Mobile Computing and Networking 2001*, pp. 272-286, July 2001.

Sivalingam, K. M., "Tutorial on Wireless Sensor Network Protocols," International Conference on High-Performance Computing 2002, Bangalore, India, December 2002.

Sohrabi, K., Gao, J., Ailawadhi, V. and Pottie, G. J., "Protocols for Self Organization of a Wireless Sensor Network," IEEE Personal Communications Magazine, vol. 7, no. 5, pp. 16-27, October 2002.

Stallings, W., Data & Computer Communications, Fifth Edition, Prentice Hall, Upper Saddle River, New Jersey, 1996.

Wang, Q., Hassanein, H. and Xu, K. (2005). A Practical Perspective on Wireless Sensor Networks. In Ilayas, M., Mahgoub, I.. (Eds.) Handbook of Sensor Networks:

Woo, A. and Culler, D., "A Transmission Control Scheme for Media Access in Sensor Networks," *Proceedings of Association for Computer Machinery Mobile Communications and Networking 2001*, pp. 221-235, July 2001.

Zhao, F. and Guibas, L. (2004). Wireless Sensor Networks: An Information Processing Approach. San Francisco.

Zhu, S., Setia, S. and Jajodia, S., "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," *Proceedings of Association for Computing Machinery Conference on Computer and Communications Security 2003,* pp. 62-72, October 2003.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dr. Gurminder Singh
   Naval Postgraduate School
   Monterey, California

4. Mr. James Ehlert
   Naval Postgraduate School
   Monterey, California

5. LTC Alejandro (Andy) Hernandez
   Naval Postgraduate School
   Monterey, California

6. LtCol Karl Pfeiffer
   Naval Postgraduate School
   Monterey, California

7. Rita Painter
   Naval Postgraduate School
   Monterey, California

8. Dr. Bruce Whalen
   SPAWARSYSCEN
   San Diego, California

9. Ivan Cardenas
   Kestrel Technology Group
   Houston, Texas

10. Thomas Latta
    Space and Naval Warfare Systems Command
    San Diego, California

11. CAPT Phil Erdie
    US Marine Corps Systems Command
    Quantico, Virginia

12. Dr. Dan C Boger
Naval Postgraduate School
Monterey, CA

13. Mr. Curtis White
USAF Force Protection Battle Lab
Lackland AFB, Texas

14. Colonel Thomas Lee Williams
U.S. Pacific Command (USPACOM)
Camp Smith, Hawaii

15. Mr. Kurt Badescher
US Special Operations Command (USSOCOM)
Tampa, Florida

16. Dr. Leonard Ferrari
Naval Postgraduate School
Monterey, California

17. Dr. Frank Shoup
Naval Postgraduate School
Monterey, California

18. Mr. Robert Sandoval
Joint Intelligence Operations Command (JIOC)
San Antonio, Texas

19. Mr. Craig Shultz
Lawrence Livermore Laboratories (LLNL)
Livermore, California

20. Group Captain Wanchai Tosuwan
Director, Research & Development Promotion Division
5th Floor A1 Muangthong Thanee
47/433 Moo 3, Banmai
Parkred, Nonthaburi, 11120

21. Group Captain Dr. Triroj Virojtriratana
DRDO COASTS Project Manager
5th Floor A1 Muangthong Thanee
47/433 Moo 3, Banmai
Parkred, Nonthaburi, 11120